IN THE CLAIMS

Please substitute claims 1-209 with the following:

1. (Currently Amended) A data providing system for distributing content data from a data providing apparatus to a data processing apparatus, wherein

said data providing apparatus distributes a module storing the content data encrypted by using content key data, encrypted content key data, and an encrypted usage control policy data indicating handling of said content data to said data processing apparatus and

said data processing apparatus decrypts said content key data and said usage control policy data stored in said distributed module and determines the handling of said content data based on the related decrypted usage control policy data,

wherein said data providing apparatus performs mutual authentication with said data processing apparatus, encrypts said module using session key data obtained by said mutual authentication, and transmits said encrypted module to said data processing apparatus,

wherein a management apparatus manages said data providing apparatus and said data processing apparatus,

wherein said data providing apparatus sends said usage control policy data and requests said management apparatus to certify legitimacy of said usage control policy data and said management apparatus registers and services said usage control policy data from said data providing apparatus, and certifies the legitimacy of said usage control policy data in response to a request from said data providing apparatus.

2. (Original) A data providing system as set forth in claim 1, wherein:

said data providing apparatus distributes said module storing said content key data and said usage control policy data encrypted using distribution key data to said data processing apparatus and

said data processing apparatus decrypts said content key data and said usage control policy data stored in said distributed module using said distribution key data.

3. (Previously Presented) A data providing system as set forth in claim 2, wherein said management apparatus manages said distribution key data and distributes said distribution key data to said data providing apparatus and said data processing apparatus.

4. (Original) A data providing system as set forth in claim 1, wherein said data providing apparatus generates its own signature data for at least one of said content key data and said usage control policy and distributes said module storing said generated signature data to said data processing apparatus.

5. (Original) A data providing system as set forth in claim 4, wherein said data providing apparatus generates said signature data using its own secret key data and distributes said module storing public key data corresponding to said secret key data to said data processing apparatus.

6. (Previously Presented) A data providing system as set forth in claim 5,

wherein said management apparatus prepares public key certificate data certifying the legitimacy of said public key data, wherein

said data providing apparatus distributes said module storing said public key certificate data to said data processing apparatus.

7. (Original) A data providing system as set forth in claim 1, wherein said data providing apparatus distributes

a first file storing said content data and

a second file storing said content key data and said usage control policy

to said data processing apparatus.

8. (Original) A data providing system as set forth in claim 7, wherein said data providing apparatus generates signature data using its own secret key data for the first file and the second file and distributes said module storing said generated signature data to said data processing apparatus.

9. (Original) A data providing system as set forth in claim 8, wherein said data processing apparatus distributes said module storing public key data corresponding to said secret key data to said data processing apparatus.

10. (Cancelled).

11. (Original) A data providing system as set forth in claim 1, wherein said data providing apparatus generates a storage medium storing said module.

12. (Original) A data providing system as set forth in claim 1, wherein said data processing apparatus determines at least one of a purchase mode and usage mode of said content data based on said usage control policy.

13. (Original) A data providing system as set forth in claim 1, wherein said data processing apparatus outputs said decrypted content key data and said encrypted content data to a decryption apparatus.

14. (Original) A data providing system as set forth in claim 9, wherein said data processing apparatus verifies the legitimacy of signature data stored in said module using public key data stored in said module.

15. (Original) A data providing system as set forth in claim 3, wherein:

said data processing apparatus determines at least one of a purchase mode and usage mode of distributed content data based on usage control policy data and transmits log data indicating a log of at least said determined purchase mode and usage mode and

said management apparatus performs profit distribution processing for distributing profit obtained accompanied with said purchase and said usage of said content data in said data processing apparatus to related parties of said data providing apparatus based on said received log data.

16. (Original) A data providing system as set forth in claim 1, wherein said data processing apparatus is comprised of a module making it difficult for the processing content, predetermined data stored in an internal memory, and data being processed from being monitored and tampered with from the outside.

17. (Currently Amended) A data processing apparatus utilizing content data distributed from a data providing apparatus, which

receives a module storing content data encrypted by using content key data, encrypted content key data, and encrypted usage control policy data indicating the handling of said content data from said data providing apparatus, decrypts said content key data and said usage control policy data stored in the related received module, and determines the handling of said content data based on the related decrypted usage control policy data

wherein said data providing apparatus performs mutual authentication with said data processing apparatus, encrypts said module using session key data obtained by said mutual authentication, and transmits said encrypted module to said data processing apparatus.

18. (Currently Amended) A data providing system comprising:

a data providing apparatus that provides a first module storing content data encrypted by using content key data, encrypted content key data, and encrypted usage control policy data indicating the handling of said content data to said data distribution apparatus,

a data distribution apparatus that distributes a second module storing said encrypted content data, content key data, and usage control policy data stored in said provided first module to said data processing apparatus,

a data processing apparatus that decrypts said content key data and said usage control policy data stored in said distributed second module and determines the handling of said content data based on the related decrypted usage control policy data, and

a management apparatus that manages said data providing apparatus and said data processing apparatus,

wherein said data distribution apparatus performs mutual authentication with said data processing apparatus, encrypts said second module using session key data obtained by said mutual authentication, and transmits said encrypted second module to said data processing apparatus,

wherein said data providing apparatus sends said usage control policy data and requests to said management apparatus to certify legitimacy of said usage control policy data, and wherein said management apparatus registers and serves said usage control policy data from said

data providing apparatus, and certifies the legitimacy of said usage control policy data in response to a request from said data providing apparatus.

19. (Original) A data providing system as set forth in claim 18, wherein said data distribution apparatus distributes a module storing price data showing a price of said content data to said data processing apparatus.

20. (Original) A data providing system as set forth in claim 18, wherein:

said data providing apparatus provides said first module storing said content key data and said usage control policy data encrypted using distribution key data to said data distribution apparatus and

said data processing apparatus decrypts said content key data and said usage control policy data stored in said distributed second module using said distribution key data.

21. (Previously Presented) A data providing system as set forth in claim 20, wherein said management apparatus manages said distribution key data and distributes said distribution key data to said data providing apparatus and said data processing apparatus.

22. (Original) A data providing system as set forth in claim 20, wherein

said data providing apparatus generates its own signature data for at least one of said content key data and said usage control policy and provides said first module storing said generated signature data and storing a third module encrypted using said distribution key data to said data distribution apparatus and

said data distribution apparatus stores said provided third module in said second module and distributes it to said data processing apparatus.

23. (Original) A data providing system as set forth in claim 22, wherein said data providing apparatus generates said signature data using its own secret key data and provides said third module storing public key data corresponding to said secret key data to said data distribution apparatus.

24. (Previously Presented) A data providing system as set forth in claim 23,

wherein said management apparatus prepares public key certificate data certifying the legitimacy of said public key data, wherein

said data providing apparatus provides said first module storing said third module storing said public key certificate data to said data distribution apparatus.

25. (Original) A data providing system as set forth in claim 18, wherein said data providing apparatus provides

a first file storing said content data and

a second file storing said content key data and said usage control policy

to said data distribution apparatus.

26. (Original) A data providing system as set forth in claim 25, wherein said data providing apparatus generates signature data using its own secret key data for the first file and the second file and provides said first module storing said generated signature data to said data distribution apparatus.

27. (Original) A data providing system as set forth in claim 25, wherein said data processing apparatus provides said first module storing public key data corresponding to said secret key data to said data distribution apparatus.

28. (Original) A data providing system as set forth in claim 19, wherein said data distribution apparatus generates signature data using its own secret key data for said price data and stores said signature data in said second module.

29. (Original) A data providing system as set forth in claim 28, wherein said data providing apparatus provides said second module storing public key data corresponding to its own secret key data to said data processing apparatus.

30. (Original) A data providing system as set forth in claim 26, wherein said data distribution apparatus verifies the signature data of said first file and said second file using public key data of said data providing apparatus.

31. (Original) A data providing system as set forth in claim 25, wherein said data providing apparatus provides said first module storing link data showing a linkage of said first file and said second file to said data distribution apparatus.

32. (Cancelled).

33. (Original) A data providing system as set forth in claim 18, wherein said data providing apparatus generates a storage medium storing said module.

34. (Original) A data providing system as set forth in claim 18, wherein said data processing apparatus determines at least one of a purchase mode and usage mode of said content data based on said usage control policy.

35. (Original) A data providing system as set forth in claim 18, wherein said data processing apparatus outputs said decrypted content key data and said encrypted content data to a decryption apparatus.

36. (Original) A data providing system as set forth in claim 29, wherein said data processing apparatus verifies the legitimacy of signature data stored in said second module using public key data stored in said second module.

37. (Original) A data providing system as set forth in claim 21, wherein:

said data processing apparatus determines at least one of a purchase mode and usage mode of distributed content data based on usage control policy data and transmits log data indicating a log of at least said determined purchase mode and usage mode and

said management apparatus performs profit distribution processing for distributing profit obtained accompanied with said purchase and said usage of said content data in said data processing apparatus to related parties of said data providing apparatus based on said received log data.

38. (Original) A data providing system as set forth in claim 18, wherein said data processing apparatus is comprised of a module making it difficult for the processing content, predetermined data stored in an internal memory, and data being processed from being monitored and tampered with from the outside.

39. (Currently Amended) A data providing system comprising:

a data providing apparatus that provides a first module storing content data encrypted by using content key data, encrypted content key data, and encrypted usage control policy data indicating the handling of said content data to said plurality of data distribution apparatuses,

a first data distribution apparatus that distributes the second module storing said encrypted content data, content key data, and usage control policy data stored in said provided first module to said data processing apparatus,

a second data distribution apparatus that distributes a third module storing said encrypted content data, content key data, and usage control policy data stored in said provided first module to said data processing apparatus,

a data processing apparatus that decrypts said content key data and said usage control policy data stored in said distributed second module and said third module and determines the handling of said content data based on the related decrypted usage control policy data, and

a management apparatus that manages said data providing apparatus and said data processing apparatus,

wherein said data distribution apparatus performs mutual authentication with said data processing apparatus, encrypts said second module using session key data obtained by said mutual authentication, and transmits said encrypted second module to said data processing apparatus,

wherein said data providing apparatus sends said usage control policy data and requests to said management apparatus to certify legitimacy of said usage control policy data, and wherein said management apparatus registers and serves said usage control policy data from said data providing apparatus, and certifies the legitimacy of said usage control policy data in response to a request from said data providing apparatus.

40. (Currently Amended) A data providing system comprising:

a first data providing apparatus that provides a first module storing first content data encrypted by using first content key data, encrypted first content key data, and encrypted first usage control policy data indicating the handling of said first content data to said data distribution apparatus,

a second data providing apparatus that provides a second module storing second content data encrypted by using second content key data, encrypted second content key data, and encrypted second usage control policy data indicating the handling of said second content data to said data distribution apparatus,

a data distribution apparatus that distributes a third module storing said encrypted first content data, said first content key data, and said first usage control policy data stored in said provided first module and said encrypted second content data, said second content key data, and said second usage control policy data stored in said provided second module to said data processing apparatus,

a data processing apparatus that decrypts said first content key data and said first usage control policy data stored in said distributed third module, determines the handling of said first content data based on the related decrypted first usage control policy data, decrypts said second content key data and said second usage control policy data stored in said distributed third module, and determines the handling of said second content data based on the related decrypted second usage control policy data, and

a management apparatus that manages said first data providing apparatus and said data processing apparatus,

wherein said data distribution apparatus performs mutual authentication with said data processing apparatus, encrypts said second module using session key data obtained by said mutual authentication, and transmits said encrypted second module to said data processing apparatus,

wherein said first data providing apparatus sends said first usage control policy data and requests to said management apparatus to certify legitimacy of said first usage control policy data, and wherein said management apparatus registers and serves said first usage control policy data from said first data providing apparatus, and certifies the legitimacy of said first usage control policy data in response to a request from said first data providing apparatus.

41. (Currently Amended) A data providing apparatus for distributing content data to a data processing apparatus for using the content data, which

distributes a module storing content data encrypted by using the content key data, encrypted content key data, and encrypted usage control policy data indicating the handling of said content data to said data processing apparatus

wherein the data providing apparatus performs mutual authentication with said data processing apparatus, encrypts said module using session key data obtained by said mutual authentication, and transmits said encrypted module to said data processing apparatus.

42. (Original) A data providing apparatus as set forth in claim 41 preparing said usage control policy and distributing said module storing said generated usage control policy to said data processing apparatus.

43. (Original) A data providing apparatus as set forth in claim 41, which distributes said module storing said content key data and said usage control policy data encrypted using distribution key data to said data processing apparatus.

44. (Original) A data providing apparatus as set forth in claim 43, which encrypts said content key data Kc and said usage control policy data using said distribution key data issued by a predetermined authority manager.

45. (Original) A data providing apparatus as set forth in claim 41, which generates its own signature data for at least one of said content data, content key data, and usage control policy data and distributes said module storing said generated signature data to said data processing apparatus.

46. (Original) A data providing apparatus as set forth in claim 45, which generates said signature data using its own secret key data and distributes said module storing public key data corresponding to said secret key data to said data processing apparatus.

47. (Original) A data providing apparatus as set forth in claim 46, which distributes said module storing public key certificate data certifying the legitimacy of said public key data to said data processing apparatus.

48. (Original) A data providing apparatus as set forth in claim 41, which distributes:

a first file storing said content data and

a second file storing said content key data and said usage control policy data

to said data processing apparatus.

49. (Original) A data providing apparatus as set forth in claim 48, which generates signature data using its own secret key data for said first file and said second file and distributes said module storing said generated signature data to said data processing apparatus.

50. (Original) A data providing apparatus as set forth in claim 49, which distributes said module storing public key data corresponding to said secret key data to said data processing apparatus.

51. (Cancelled).

52. (Original) A data providing apparatus as set forth in claim 41, which generates a storage medium storing said module.

53. (Original) A data providing apparatus as set forth in claim 41, which defines said module by an application layer.

54. (Original) A data providing apparatus as set forth in claim 53, which uses a presentation layer and transport layer under said application layer as distribution protocol for distributing said module to said data processing apparatus.

55. (Original) A data providing apparatus as set forth in claim 41, which defines said module by a format not dependent on a medium for distributing said module to said data processing apparatus.

56. (Currently Amended) A data providing method for distributing data from a data providing apparatus to a data processing apparatus, comprising the steps of:

distributing a module storing content data encrypted by using content key data, encrypted content key data, and encrypted usage control policy data indicating the handling of said content data from said data providing apparatus to said data processing apparatus

performing mutual authentication with said data processing apparatus, encrypting said module using session key data obtained by said mutual authentication, and transmitting said encrypted module to said data processing apparatus and

decrypting said content key data and said usage control policy data stored in said distributed module and determining the handling of said content data based on the related decrypted usage control policy data at said data processing apparatus.

57. (Original) A data providing method as set forth in claim 56, further comprising the steps of:

distributing said module storing said content key data and said usage control policy data encrypted using distribution key data from said data providing apparatus to said data processing apparatus and

decrypting said content key data and said usage control policy stored in said distributed module using said distribution key data.

58. (Currently Amended) A data providing method using a data providing apparatus, data distribution apparatus, and data processing apparatus, comprising the steps of:

providing a first module storing content data encrypted by using content key data, encrypted content key data, and encrypted usage control policy data indicating the handling of said content data from said data providing apparatus to said data distribution apparatus,

distributing a second module storing said encrypted content data, content key data, and usage control policy data stored in said provided first module from said data distribution apparatus to said data processing apparatus

performing mutual authentication with said data processing apparatus, encrypting said module using session key data obtained by said mutual authentication, and transmitting said encrypted module to said data processing apparatus, and

decrypting said content key data and said usage control policy data stored in said distributed second module and determining the handling of said content data based on the related decrypted usage control policy data at said data processing apparatus.

59. (Original) A data providing method as set forth in claim 58, which distributes said second module storing price data showing a price of said content data from said data distribution apparatus to said data processing apparatus.

60. (Currently Amended) A data providing method using a data providing apparatus, at least a first data distribution apparatus and second data distribution apparatus, and a data processing apparatus, comprising the steps of:

providing a first module storing content data encrypted by using content key data, encrypted content key data, and encrypted usage control policy data indicating the handling of said content data from said data providing apparatus to said data distribution apparatuses,

distributing a second module storing said encrypted content data, content key data, and usage control policy data stored in said provided first module from said first data distribution apparatus to said data processing apparatus,

distributing a third module storing said encrypted content data, content key data, and usage control policy data stored in said provided first module from said second data distribution apparatus to said data processing apparatus

performing mutual authentication with said data processing apparatus, encrypting said module using session key data obtained by said mutual authentication, and transmitting said encrypted module to said data processing apparatus, and

decrypting said content key data and said usage control policy data stored in said distributed second module and said third module and determining the handling of said content data based on the related decrypted usage control policy data at said data processing apparatus.

61. (Currently Amended) A data providing method using at least a first data providing apparatus and second data providing apparatus, a data distribution apparatus, and a data processing apparatus, comprising the steps of:

providing a first module storing first content data encrypted by using first content key data, encrypted first content key data, and encrypted first usage control policy data indicating the handling of said first content data from said first data providing apparatus to said data distribution apparatus,

providing a second module storing second content data encrypted by using second content key data, encrypted second content key data, and encrypted second usage control policy data indicating the handling of said second content data from said second data providing apparatus to said data distribution apparatus,

distributing a third module storing said encrypted first content data, said first content key data, and said first usage control policy data stored in said provided first module and said encrypted second content data, said second content key data, and said second usage control policy data stored in said provided second module from said data distribution apparatus to said data processing apparatus

performing mutual authentication with said data processing apparatus, encrypting said module using session key data obtained by said mutual authentication, and transmitting said encrypted module to said data processing apparatus, and

decrypting said first content key data and said first usage control policy data stored in said distributed third module, determining the handling of said first content data based on the related decrypted first usage control policy data, decrypting said second content key data and

said second usage control policy data stored in said distributed third module, and determining the handling of said second content data based on the related decrypted second usage control policy data at said data processing apparatus

62. (Currently Amended) A data providing method for distributing content data to a data processing apparatus using said content data, which

distributes a module storing content data encrypted using content key data, said encrypted content key data, and encrypted usage control policy data showing the handling of said content data

performing mutual authentication with said data processing apparatus, encrypting said module using session key data obtained by said mutual authentication, and transmitting said encrypted module to said data processing apparatus.

63. (Original) A data providing method as set forth in claim 62, which distributes said module storing said content key data and said usage control policy data encrypted using distribution key data to said data processing apparatus.

64. (Original) A data providing method as set forth in claim 62, which generates its own signature data for at least one of said content data, said content key data, and said usage control policy data and distributes said module storing said generated signature data to said data processing apparatus.

65. (Original) A data providing method as set forth in claim 64, which generates said signature data using its own secret key data and distributes said module storing public key data corresponding to said secret key data to said data processing apparatus.

66. (Original) A data providing method as set forth in claim 65, which distributes said module storing public key certificate data certifying the legitimacy of said public key data to said data processing apparatus.

67. (Original) A data providing method as set forth in claim 62, which distributes:

a first file storing said content data and

a second file storing said content key data and said usage control policy data

to said data processing apparatus.

68. (Original) A data providing method as set forth in claim 67, which generates signature data using its own secret key data for said first file and said second file and stores said generated signature data.

69. (Original) A data providing method as set forth in claim 68, which distributes a module storing public key data corresponding to said secret key data to said data processing apparatus.

70. (Cancelled).

71. (Original) A data providing method as set forth in claim 62, which generates a storage medium storing said module.

72. (Currently Amended) A data providing system comprising:

a data providing apparatus that distributes content data and usage control policy data indicating the handling of the related content data to said data processing apparatus,

a data processing apparatus that uses said distributed content data based on said distributed usage control policy data, and

a management apparatus that manages said data providing apparatus and said data processing apparatus,

wherein said data providing apparatus performs mutual authentication with said data processing apparatus, encrypts said module using session key data obtained by said mutual authentication, and transmits said encrypted module to said data processing apparatus,

wherein said data providing apparatus sends said usage control policy data and requests to said management apparatus to certify legitimacy of said usage control policy data, and wherein said management apparatus registers and serves said usage control policy data from said data providing apparatus, and certifies the legitimacy of said usage control policy data in response to a request from said data providing apparatus.

73. (Original) A data providing system as set forth in claim 72, wherein said data providing apparatus makes said request by transmitting to said management apparatus a module storing said usage control policy data, its own identifier, and signature data generated using its own secret key data for at least said usage control policy data.

74. (Original) A data providing system as set forth in claim 73, wherein

said management apparatus distributes public key certificate data for certifying the legitimacy of the public key data corresponding to said secret key data of said data providing apparatus to said data providing apparatus together with the signature data generated by using its own secret key data, and

said data providing apparatus makes a request by transmitting a module storing said public key certificate data, said usage control policy data, its own identifier, and said signature data to said management apparatus.

75. (Original) A data providing system as set forth in claim 72, wherein:

said management apparatus manages distribution key data, distributes the related distribution key data to said data processing apparatus, generates signature data generated by using its own secret key data with respect to said usage control policy data in response to a request from said data providing apparatus, encrypts a module storing the related generated signature data and said usage control policy data by using said distribution key data, and transmits the same to said data providing apparatus,

said data providing apparatus distributes a module received from said management apparatus to said data processing apparatus, and

said data processing apparatus decrypts said module received from said data providing apparatus by using said distribution key data, verifies the legitimacy of said signature data stored in the related module by using the public key data of said management apparatus, and uses said distributed content data based on the usage control policy data stored in said module when it decides it is legitimate.

76. (Original) A data providing system as set forth in claim 72, wherein:

said data processing apparatus determines at least one of a purchase mode and usage mode of distributed content data based on usage control policy data and transmits log data indicating a log of at least said determined purchase mode and usage mode and

said management apparatus performs profit distribution processing for distributing profit obtained accompanied with said purchase and said usage of said content data in said data processing apparatus to related parties of said data providing apparatus based on said received log data.

77. (Currently Amended) A data providing system comprising:

a data providing apparatus that encrypts content data by using content key data, distributes the related encrypted content data to said data processing apparatus,

a data processing apparatus that decrypts said distributed content data by using said content key data and uses the related decrypted content data, and

a management apparatus that manages said data providing apparatus and said data processing,

wherein said data providing apparatus performs mutual authentication with said data processing apparatus, encrypts said module using session key data obtained by said mutual authentication, and transmits said encrypted module to said data processing apparatus,

wherein said data providing apparatus sends said usage control policy data and requests to said management apparatus to certify legitimacy of said usage control policy data, and wherein said management apparatus registers and serves said usage control policy data from said data providing apparatus, and certifies the legitimacy of said usage control policy data in response to a request from said data providing apparatus.

78. (Original) A data providing system as set forth in claim 77, wherein said data providing apparatus distributes a module storing said content data and said content key data to said data processing apparatus.

79. (Currently Amended) A management apparatus for managing a data providing apparatus for distributing content data and usage control policy data indicating the handling of the related content data and a data processing apparatus for using said distributed content data based on said distributed usage control policy data, which

registers and serves said usage control policy data from said data providing apparatus, and certifies the legitimacy of said usage control policy data in response to a request from said data providing apparatus

wherein said data providing apparatus performs mutual authentication with said data processing apparatus, encrypts a module using session key data obtained by said mutual authentication, and transmits said encrypted module to said data processing apparatus.

80. (Original) A data providing system as set forth in claim 79, which manages public key data corresponding to secret key data of said data providing apparatus when receiving from said data providing apparatus said request using a module storing said usage control policy data, an identifier of said data providing apparatus, and signature data generated using secret key data of said data providing apparatus for at least said usage control policy data.

81. (Original) A data providing system as set forth in claim 80, which transmits public key certificate data certifying the legitimacy of said public key data to said data providing apparatus.

82. (Currently Amended) A management apparatus for managing a data providing apparatus for distributing content data and usage control policy data indicating the handling of the related content data encrypted using content key data and a data processing apparatus for using said distributed content data after decrypting said distributed content data using said content key data based on said distributed usage control policy data, which

registers and serves said usage control policy data from said data providing apparatus, and certifies the legitimacy of said content key data in response to a request from said data providing apparatus

wherein said data providing apparatus performs mutual authentication wi`th said data processing apparatus, encrypts said module using session key data obtained by said mutual authentication, and transmits said encrypted module to said data processing apparatus.

83. (Currently Amended) A data providing system comprising:

a data providing apparatus that provides content data and usage control policy data indicating the handling of the related content data to said data distribution apparatus

a data distribution apparatus that distributes said provided content data and said usage control policy data to said data processing apparatus,

a data processing apparatus that uses said distributed content data based on said distributed usage control policy data, and

a management apparatus that manages said data providing apparatus and said data processing apparatus,

wherein said data providing apparatus performs mutual authentication with said data processing apparatus, encrypts said module using session key data obtained by said mutual authentication, and transmits said encrypted module to said data processing apparatus,

wherein said data providing apparatus sends said usage control policy data and requests to said management apparatus to certify legitimacy of said usage control policy data, and wherein said management apparatus registers and serves said usage control policy data from said data providing apparatus, and certifies the legitimacy of said usage control policy data in response to a request from said data providing apparatus.

84. (Original) A data providing system as set forth in claim 83, wherein said data providing apparatus makes said request by transmitting to said management apparatus a module

storing an identifier of said content data, said usage control policy data, and signature data generated using its own secret key data for at least said usage control policy data.

85. (Original) A data providing system as set forth in claim 84, wherein said management apparatus distributes public key certificate data certifying the legitimacy of public key data corresponding to said secret key data of said data providing apparatus together with signature data generated using its own secret key data to said data providing apparatus.

86. (Original) A data providing system as set forth in claim 84, wherein said

said management apparatus manages distribution key data, distributes the related distribution key data to said data processing apparatus, generates signature data generated by using its own secret key data with respect to said usage control policy data in response to a request from said data providing apparatus, encrypts a module storing the related generated signature data and said usage control policy data by using said distribution key data, and transmits the same to said data providing apparatus,

said data providing apparatus distributes a module received from said management apparatus to said data distribution apparatus, and

said data processing apparatus decrypts said module distributed said data distribution apparatus, verifies the legitimacy of said signature data stored in the related module by using the public key data of said management apparatus, and uses said distributed content data based on the usage control policy data stored in said module when it decides it is legitimate.

87. (Original) A data providing system as set forth in claim 83, wherein:

said data distribution apparatus distributes price data indicating the price of said distributed content data to said data processing apparatus and

said management apparatus certifies the legitimacy of said price data in response to a request from said data distribution apparatus.

88. (Original) A data providing system as set forth in claim 83, wherein

said data processing apparatus determines at least one of a purchase mode and usage mode of distributed content data based on said usage control policy data and transmits log data indicating a log of at least said determined purchase mode and usage mode to said management apparatus and

said management apparatus performs profit distribution processing for distributing profit obtained accompanied with said purchase and said usage of said content data in said data processing apparatus to related parties of said data providing apparatus and said data distribution apparatus based on said received log data.

89. (Original) A data providing system as set forth in claim 83, wherein

said data processing apparatus has a first module communicating with said data distribution apparatus and a second module determining at least one of a purchase mode and usage mode of distributed content data based on said distributed usage control policy data and transmitting log data indicating a log of at least said determined purchase mode and usage mode to said management apparatus and

said management apparatus manages the data providing apparatus, data distribution apparatus, and data processing apparatus and performs profit distribution processing for distributing profit obtained accompanied with said data processing apparatus receiving distribution of said content data and purchasing and using said content data to related parties of

said data providing apparatus and said data distribution apparatus based on said received log data received from said second module.

90. (Currently Amended) A data providing system comprising:

a data providing apparatus that encrypts content data by using content key data, provides related encrypted content data, and usage control policy data indicating the handling of the related content data to said data distribution apparatus,

a data distribution apparatus that distributes said provided content data and said usage control policy data to said data processing apparatus,

a data processing apparatus that uses said content data containing the decryption of said content data using said content key data based on said distributed usage control policy data, and

a management apparatus that manages said data providing apparatus and said data processing apparatus,

wherein said data providing apparatus performs mutual authentication with said data processing apparatus, encrypts said module using session key data obtained by said mutual authentication, and transmits said encrypted module to said data processing apparatus,

wherein said data providing apparatus requests to said management apparatus to certify legitimacy of said content key data, and wherein said management apparatus registers and serves said usage control policy data from said data providing apparatus, and certifies the legitimacy of said content key data in response to a request from said data providing apparatus.

91. (Original) A data providing system as set forth in claim 90, wherein said data providing apparatus encrypts said content key data and provides a module storing said encrypted content key data and encrypted content data to said data distribution apparatus.

92. (Currently Amended) A management apparatus for managing a data providing apparatus for providing content data and usage control policy data indicating the handling of the related content data, a data distribution apparatus for distributing said provided content data and said usage control policy data, and a data processing apparatus for using said distributed content data based on said distributed usage control policy data, which

registers and serves said usage control policy data from said data providing apparatus, and certifies the legitimacy of said usage control policy data in response to a request from said data providing apparatus

wherein said data providing apparatus performs mutual authentication with said data processing apparatus, encrypts said module using session key data obtained by said mutual authentication, and transmits said encrypted module to said data processing apparatus.

93. (Original) A management apparatus as set forth in claim 92, which certifies the legitimacy of said content key data in response to a request from said data providing apparatus when encrypting said content data using content key data and providing it from said data providing apparatus to said data distribution apparatus.

94. (Original) A management apparatus as set forth in claim 92, which certifies the legitimacy of said price data in response to a request from said data distribution apparatus when distributing said price data from said data distribution apparatus to said data processing apparatus together with said content data and said usage control policy data.

95. (Currently Amended) A data providing method using a data providing apparatus, data processing apparatus, and management apparatus, comprising the steps of:

distributing content data and usage control policy data indicating the handling of the related content data from said data providing apparatus to said data processing apparatus,

using said distributed content data based on said distributed usage control policy data at said data processing apparatus,

registering and serving said usage control policy data from said data providing apparatus, ~~and~~

certifying the legitimacy of said usage control policy data in said management apparatus in response to a request from said data providing apparatus, and

performing mutual authentication with said data processing apparatus, encrypting said module using session key data obtained by said mutual authentication, and transmitting said encrypted module to said data processing apparatus.

96. (Currently Amended) A data providing method using a data providing apparatus, data processing apparatus, and management apparatus, comprising the steps of:

distributing content data encrypted by using content key data from said data providing apparatus to said data processing apparatus,

decrypting said distributed content data by using said content key data at said data processing apparatus,

registering and serving said usage control policy data from said data providing apparatus, ~~and~~

certifying the legitimacy of said content key data in said management apparatus in response to a request from said data providing apparatus, and

performing mutual authentication with said data processing apparatus, encrypting said module using session key data obtained by said mutual authentication, and transmitting said encrypted module to said data processing apparatus.

97. (Currently Amended) A data providing method using a data providing apparatus, data distribution apparatus, data processing apparatus, and management apparatus, comprising the steps of:

providing content data and usage control policy data indicating the handling of the related content data from said data providing apparatus to said data distribution apparatus,

distributing said provided content data and said usage control policy data from said data distribution apparatus to said data processing apparatus,

using said distributed content data based on said distributed usage control policy data at said data processing apparatus,

registering and serving said usage control policy data from said data providing apparatus, ~~and~~

certifying the legitimacy of said usage control policy data in said management apparatus in response to a request from said data providing apparatus, and

performing mutual authentication with said data processing apparatus, encrypting said module using session key data obtained by said mutual authentication, and transmitting said encrypted module to said data processing apparatus.

98. (Currently Amended) A data providing method using a data providing apparatus, data distribution apparatus, data processing apparatus, and management apparatus, comprising the steps of:

providing content data encrypted by using content key data and usage control policy data indicating the handling of the related content data from said data providing apparatus to said data distribution apparatus,

performing mutual authentication with said data processing apparatus, encrypting said module using session key data obtained by said mutual authentication, and transmitting said encrypted module to said data processing apparatus

distributing said content data and said usage control policy data provided from said data distribution apparatus to said data processing apparatus to said data processing apparatus,

using said content data containing the decryption of said content data using said content key data based on said distributed usage control policy data in said data processing apparatus,

registering and serving said usage control policy data from said data providing apparatus, and

certifying the legitimacy of said content key data in said management apparatus in response to a request from said data providing apparatus.

99. (Currently Amended) A data providing system comprising:

a data providing apparatus that distributes content data and usage control policy data indicating the handling of the related content data to said data processing apparatus,

a data processing apparatus that determines at least one of a purchase mode and a usage mode of said distributed content data based on said distributed usage control policy data and

transmits log data indicating the log of at least one of the related determined purchase mode and usage mode to said management apparatus, and

a management apparatus that manages said data providing apparatus and said data processing apparatus and performs profit distribution processing for distributing the profit obtained accompanied with said purchase and said usage of said content data in said data processing apparatus to related parties of said data providing apparatus based on received log data,

wherein said data providing apparatus performs mutual authentication with said data processing apparatus, encrypts said module using session key data obtained by said mutual authentication, and transmits said encrypted module to said data processing apparatus,

wherein said data providing apparatus sends said usage control policy data and requests to said management apparatus to certify legitimacy of said usage control policy data, and wherein said management apparatus registers and serves said usage control policy data from said data providing apparatus, and certifies the legitimacy of said usage control policy data in response to a request from said data providing apparatus.

100. (Original) A data providing system as set forth in claim 99, wherein

said data providing apparatus encrypts said content data using predetermined key data and distributes it to said data processing apparatus,

said data processing apparatus decrypts said received content data using said key data, and

said management apparatus manages said key data.

101. (Original) A data providing system as set forth in claim 99, wherein

said data providing apparatus generates predetermined key data and registers said generated key data to said management apparatus,

said management apparatus manages said registered key data and transmits corresponding key data to said data processing apparatus when processing for purchasing of content data is performed in said data processing apparatus, and

said data processing apparatus decrypts said received content data using said received key data.

102. (Original) A data providing system as set forth in claim 100, wherein said data providing apparatus encrypts said key data and distributes a module storing said encrypted key data, encrypted content data, and said usage control policy data to said data processing apparatus.

103. (Original) A data providing system as set forth in claim 102, wherein

said management apparatus manages distribution key data and distributes said distribution key data to said data providing apparatus and said data processing apparatus,

said data providing apparatus encrypts said key data and said usage control policy data using said distributed distribution key data, and

said data processing apparatus decrypts said key data and said usage control policy data using said distributed distribution key data.

104. (Original) A data providing system as set forth in claim 103, wherein said management apparatus distributes a plurality of distribution key data having predetermined terms of validity to said data providing apparatus and said data processing apparatus for exactly a predetermined period.

105. (Original) A data providing system as set forth in claim 102, wherein

said data providing apparatus generates signature data for at least one of said encrypted content data and usage control policy data using its own secret key data and distributes a module storing said encrypted content data, said encrypted key data, said encrypted usage control policy data, and said signature data to said data processing apparatus,

said data processing apparatus verifies said signature data stored in said distributed module using public key data corresponding to said secret key data, and

said management apparatus manages said public key data.

106. (Original) A data providing system as set forth in claim 105, wherein said data providing apparatus distributes said module storing public key data corresponding to its own secret key data to said data processing apparatus.

107. (Original) A data providing system as set forth in claim 105, wherein said management apparatus distributes said module storing public key data corresponding to said secret key data of said data providing apparatus to said data processing apparatus.

108. (Original) A data providing system as set forth in claim 99, wherein

said management apparatus distributes distribution key data to said data providing apparatus and said data processing apparatus,

said data providing apparatus encrypts said usage control policy using said distribution key data and distributes it to said data processing apparatus, and

said data processing apparatus decrypts said received usage control policy data using said distribution key data.

109. (Original) A data providing system as set forth in claim 100, wherein said management apparatus authenticates the legitimacy of at least one of said usage control policy data and said key data.

110. (Original) A data providing system as set forth in claim 99, wherein said management apparatus generates settlement claim data used when claiming settlement processing in accordance with said profit distribution processing, adds signature data based on its own secret key data to said settlement claim data, and transmits it to an apparatus performing said settlement processing or said data providing apparatus.

111. (Original) A data providing system as set forth in claim 99, wherein said management apparatus performs processing for registration of said data processing apparatus, manages said registered data processing apparatus, and performs profit distribution processing based on said log data received from said registered data processing apparatus.

112. (Original) A data providing system as set forth in claim 99, wherein said data processing apparatus determines a purchase mode of said distributed content data based on said usage control policy data, generates usage control status data in accordance with said determined purchase mode, and controls usage of said distributed content data based on said usage control status data.

113. (Original) A data providing system as set forth in claim 99, wherein said data processing apparatus is comprised of a module making it difficult for the processing content, predetermined data stored in an internal memory, and data being processed from being monitored and tampered with from the outside.

114. (Currently Amended) A management apparatus for managing a data providing apparatus for distributing content data and usage control policy data indicating the handling of said content data and a data processing apparatus for determining at least one of a purchase mode and usage mode of said distributed content data based on said distributed usage control policy data and generating log data showing a log of at least one of said determined purchase mode and usage mode, which

receives said log data from said data processing apparatus and performs profit distribution processing for distributing the profit accompanied with said purchase and said usage of said content data in said data processing apparatus to related parties of said data providing apparatus based on said received log data,

wherein said data providing apparatus performs mutual authentication with said data processing apparatus, encrypts said module using session key data obtained by said mutual authentication, and transmits said encrypted module to said data processing apparatus,

wherein said management apparatus registers and serves said usage control policy data from said data providing apparatus, and certifies the legitimacy of said usage control policy data in response to a request from said data providing apparatus.

115. (Original) A management apparatus as set forth in claim 113, which manages key data when distributing content data encrypted using predetermined key data from said data providing apparatus to said data processing apparatus.

116. (Original) A management apparatus as set forth in claim 114, which authenticates the legitimacy of at least one of said usage control policy data and key data used when decrypting said content data.

117. (Currently Amended) A data providing apparatus for receiving distribution of content data and usage control policy data indicating the handling of the related content data from a data providing apparatus and transmitting log data to a management apparatus for performing profit distribution processing for distributing the profit obtained accompanied with the purchase and usage of the related distributed content data to related parties of said data providing apparatus based on predetermined log data, which

determines at least one of a purchase mode and usage mode of said distributed content data based on said distributed usage control policy data and transmits said log data indicating the log of the determined designation mode and usage mode to said management apparatus,

wherein said data providing apparatus performs mutual authentication with said data processing apparatus, encrypts said module using session key data obtained by said mutual authentication, and transmits said encrypted module to said data processing apparatus,

wherein said data providing apparatus sends said usage control policy data and requests to said management apparatus to certify legitimacy of said usage control policy data.

118. (Original) A data providing apparatus as set forth in claim 117, which receives said key data from said data providing apparatus when said content data is encrypted using predetermined key data.

119. (Original) A data processing apparatus as set forth in claim 117, comprised of a module making it difficult for the processing content, predetermined data stored in an internal memory, and data being processed from being monitored and tampered with from the outside.

120. (Currently Amended) A data providing system comprising:

a data providing apparatus that provides content data and usage control policy data indicating the handling of the related content data to said data distribution apparatus,

a data distribution apparatus that distributes said provided content data and said usage control policy data to said data processing apparatus,

a data processing apparatus that has a first module for communicating with said data distribution apparatus and a second module for determining at least one of a purchase mode and usage mode of said distributed content data based on said distributed usage control policy data and transmitting log data indicating the log of the related determined purchase mode and usage mode to said management apparatus, and

a management apparatus that manages the data providing apparatus, data distribution apparatus, and data processing apparatus and performs profit distribution processing for distributing the profit obtained accompanied with said data processing apparatus receiving said distribution of said content data and purchasing and using said content data to related parties of said data providing apparatus and said data distribution apparatus based on said log data received from said second module,

wherein said data providing apparatus performs mutual authentication with said data processing apparatus, encrypts said module using session key data obtained by said mutual authentication, and transmits said encrypted module to said data processing apparatus,

wherein said data providing apparatus sends said usage control policy data and requests to said management apparatus to certify legitimacy of said usage control policy data, and wherein said management apparatus registers and serves said usage control policy data from said

data providing apparatus, and certifies the legitimacy of said usage control policy data in response to a request from said data providing apparatus.

121. (Original) A data providing system as set forth in claim 120, wherein said data providing apparatus encrypts said content data using content key data and provides it to said data distribution apparatus.

122. (Original) A data providing system as set forth in claim 120, wherein said data distribution apparatus generates price data showing the price of said distributed content data and distributes said price data to said data processing apparatus.

123. (Original) A data providing system as set forth in claim 120, wherein

said data providing apparatus encrypts said content key data and said usage control policy by using distribution key data and provides it to said data distribution apparatus,

said data processing apparatus decrypts said content key data and said usage control policy using said distribution key data, and

said management apparatus manages said distribution key data and distributes said distribution key data to said data providing apparatus and said data processing apparatus.

124. (Original) A data providing system as set forth in claim 123, wherein

said data providing apparatus generates first signature data for at least one of said encrypted content data, said encrypted content key data, and said encrypted usage control policy data using its own first secret key data and provides a first module storing said encrypted content data, said encrypted key data, said encrypted usage control policy data, and said first signature data to said data distribution apparatus,

said data distribution apparatus verifies said first signature data using first public key data corresponding to said first secret key data, then stores second signature data generated using its own second secret key data in said first module to generate a second module and distributes said second module to said data processing apparatus,

said data processing apparatus verifies said first signature data stored in said distributed second module using said first public key data and verifies said second signature data stored in said distributed second module using second public key data corresponding to said second secret key data, and

said management apparatus manages said first public key data and said second public key data.

125. (Original) A data providing system as set forth in claim 124, wherein

said data providing apparatus provides said first module storing said first public key data to said data distribution apparatus and

said data distribution apparatus distributes said second module storing said first public key data and said second public key data to said data processing apparatus.

126. (Original) A data providing system as set forth in claim 124, wherein said management apparatus distributes said first public key data and said second public key data to said data processing apparatus.

127. (Original) A data providing system as set forth in claim 120, wherein

said data distribution apparatus distributes price data showing the price of said distributed content data to said data processing apparatus and

said management apparatus authenticates the legitimacy of the data of at least one of key data used when encrypting said content data and said price data.

128. (Original) A data providing system as set forth in claim 120, wherein said data distribution apparatus distributes to said data processing apparatus a module storing said provided encrypted content data, said provided usage control policy data, said key data encrypting said content data, and price data showing the price of said distributed content data.

129. (Original) A data providing system as set forth in claim 120, wherein said management apparatus performs profit distribution processing for distributing profit obtained accompanied with said data processing apparatus receiving distribution of said content data and purchasing and using said content data to related parties of said data providing apparatus and said data distribution apparatus, generates settlement claim data to be used when claiming settlement, add its own signature data to said settlement claim data, and transmits this to an apparatus for performing said settlement processing.

130. (Original) A data providing system as set forth in claim 129, wherein said management apparatus transmits settlement report data showing the results of said profit distribution processing to at least one of said data providing apparatus and said data distribution apparatus.

131. (Original) A data providing system as set forth in claim 120, wherein said management apparatus performs profit distribution processing for distributing profit obtained accompanied with said data processing apparatus receiving distribution of said content data and purchasing and using said content data to related parties of said data providing apparatus and said data distribution apparatus, generates settlement claim data to be used when claiming

settlement, adds its own signature data to said settlement claim data, and transmits this to at least one of said data providing apparatus and said service providing apparatus.

132. (Original) A data providing system as set forth in claim 120, wherein said management apparatus performs processing for registration of said data processing apparatus, manages said registered data processing apparatus, and performs said profit distribution processing based on said log data received from said registered data processing apparatus.

133. (Original) A data providing system as set forth in claim 120, wherein said data processing apparatus determines at least one of a purchase mode and usage mode of said distributed content data based on said usage control policy data, generates usage control status data in accordance with said determined purchase mode and usage mode, and controls usage of said distributed content data based on said usage control status data.

134. (Original) A data providing system as set forth in claim 120, wherein said second module of said data processing apparatus is a module making it difficult for the processing content, predetermined data stored in an internal memory, and data being processed from being monitored and tampered with from the outside.

135. (Currently Amended) A management apparatus for managing a data providing apparatus for providing content data and usage control policy data indicating the handling of the related content data, a data distribution apparatus for distributing said provided content data and said usage control policy data, and a data processing apparatus for determining at least one of a purchase mode and usage mode of said distributed content data based on said distributed usage control policy data and creating log data indicating the log of at least one of the related determined purchase mode and usage mode, which

performs profit distribution processing for distributing the profit obtained accompanied with said data processing apparatus receiving said distribution of said content data and purchasing and using said content data to related parties of said data providing apparatus and said data distribution apparatus based on said received log data,

registers and serves said usage control policy data from said data providing apparatus, and

certifies the legitimacy of said usage control policy data in response to a request from said data providing apparatus

wherein said data providing apparatus performs mutual authentication with said data processing apparatus, encrypts said module using session key data obtained by said mutual authentication, and transmits said encrypted module to said data processing apparatus.

136. (Original) A management apparatus as set forth in claim 135, which manages said key data when distributing said content data encrypted using predetermined content key data from said data providing apparatus to said data processing apparatus.

137. (Original) A management apparatus as set forth in claim 136, which authenticates the legitimacy of at least one of said usage control policy data and said content key data.

138. (Currently Amended) A data processing apparatus for receiving distribution of content data and usage control policy data from a data distribution apparatus receiving the provision of content data and usage control policy data indicating the handling of the related content data from a data providing apparatus and transmitting log data to a management apparatus for performing profit distribution processing for distributing the profit obtained accompanied with the purchase and usage of said distributed content data to related parties of

said data providing apparatus and said data distribution apparatus based on predetermined log data, which has

a first module for communicating with said data distribution apparatus and

a second module for determining at least one of a purchase mode and usage mode of said distributed content data based on said distributed usage control policy data and transmitting log data indicating the log of the related determined purchase mode and usage mode to said management apparatus,

wherein said data providing apparatus performs mutual authentication with said data processing apparatus, encrypts said first module using session key data obtained by said mutual authentication, and transmits said encrypted module to said data processing apparatus,

wherein said data providing apparatus sends said usage control policy data and requests to said management apparatus to certify legitimacy of said usage control policy data, and wherein said management apparatus registers and serves said usage control policy data from said data providing apparatus, and certifies the legitimacy of said usage control policy data in response to a request from said data providing apparatus.

139. (Original) A data processing apparatus as set forth in claim 138, which is a module making it difficult for the processing content, predetermined data stored in an internal memory, and data being processed from being monitored and tampered with from the outside.

140. (Currently Amended) A data providing system comprising:

a data providing apparatus that provides content data and usage control policy data indicating the handling of the related content data to said data distribution apparatus,

a data distribution apparatus that distributes said provided content data and said usage control policy data to said data processing apparatus and performs charge processing concerning the distribution of said content data based on a data distribution apparatus use purchase log data received from said data processing apparatus,

a data processing apparatus that has a first module for creating the data distribution apparatus use purchase log data indicating the log of the purchase of said content data distributed from said data distribution apparatus and transmitting the same to said data distribution apparatus and a second module for determining at least one of the purchase mode and the usage mode of said distributed content data based on said distributed usage control policy data and transmitting a management apparatus use log data indicating the log of the related determined purchase mode and usage mode to said management apparatus, and

a management apparatus that performs profit distribution processing for distributing the profit obtained accompanied with said purchase and said usage of said content data in said data processing apparatus to related parties of said data providing apparatus and said data distribution apparatus based on said management apparatus use log data,

wherein said data providing apparatus performs mutual authentication with said data processing apparatus, encrypts said module using session key data obtained by said mutual authentication, and transmits said encrypted module to said data processing apparatus,

wherein said data providing apparatus sends said usage control policy data and requests to said management apparatus to certify legitimacy of said usage control policy data, and wherein said management apparatus registers and serves said usage control policy data from said

data providing apparatus, and certifies the legitimacy of said usage control policy data in response to a request from said data providing apparatus.

141. (Currently Amended) A data processing apparatus for receiving the distribution of content data and usage control policy data indicating the handling of the related content data from a data providing apparatus via a data distribution apparatus and transmitting said log data to a management apparatus for performing profit distribution processing for distributing the profit obtained accompanied with the purchase and usage of the related distributed content data to related parties of said data providing apparatus and said data distribution apparatus based on said management apparatus use log data, said data processing apparatus comprising,

a first module for creating data distribution apparatus use purchase log data indicating the log of the purchase of said content data distributed from said data distribution apparatus and transmitting the same to said data distribution apparatus and

a second module for determining at least one of a purchase mode and usage mode of said distributed content data based on said distributed usage control policy data and transmitting said management apparatus use log data indicating the log of the related determined purchase mode and usage mode to said management apparatus,

wherein said data providing apparatus performs mutual authentication with said data processing apparatus, encrypts said module using session key data obtained by said mutual authentication, and transmits said encrypted module to said data processing apparatus,

wherein said data providing apparatus sends said usage control policy data and requests to said management apparatus to certify legitimacy of said usage control policy data, and wherein said management apparatus registers and serves said usage control policy data from said

data providing apparatus, and certifies the legitimacy of said usage control policy data in response to a request from said data providing apparatus.

142. (Currently Amended) A data providing system comprising:

a data providing apparatus that provides the content data to said data distribution apparatus and provides usage control policy data indicating the handling of said content data to said distribution apparatus,

a data distribution apparatus that distributes said provided content data to said data processing apparatus,

a data processing apparatus that uses said distributed content data, and

a management apparatus that manages operation of a data providing service by said data providing apparatus, said data distribution apparatus, and said data processing apparatus,

wherein said data providing apparatus performs mutual authentication with said data processing apparatus, encrypts said module using session key data obtained by said mutual authentication, and transmits said encrypted module to said data processing apparatus,

wherein said data providing apparatus sends said usage control policy data and requests to said management apparatus to certify legitimacy of said usage control policy data, and wherein said management apparatus registers and serves said usage control policy data from said data providing apparatus, and certifies the legitimacy of said usage control policy data in response to a request from said data providing apparatus.

143. (Previously Presented) A data providing system as set forth in claim 142, wherein:

said data distribution apparatus distributes said provided content data and usage control policy data to said data processing apparatus,

said data processing apparatus uses said distributed content data based on said distributed usage control policy data, and

said management apparatus plays the role of a sub-certificate authority present hierarchically under a route certificate authority, generates and manages public key certificate data to be used when certifying the legitimacy of public key data corresponding to secret key data to be used at said registered data providing apparatus, data distribution apparatus, and data processing apparatus, authenticates said usage control policy data, and performs right processing relating to said content data.

144. (Original) A data providing system as set forth in claim 143, wherein

said data providing apparatus encrypts using said key data and provides the result to said data distribution apparatus and

said management apparatus manages said key data.

145. (Original) A data providing system as set forth in claim 143, wherein

each of said data providing apparatus and said data distribution apparatus generates its own secret key data to be used for authentication with another apparatus, manages said generated secret key data, generates public key data corresponding to said secret key data, and registers said public key data, identification card, and settlement account to said management apparatus and

said management apparatus generates public key certificate data certifying the legitimacy of said public key data.

146. (Original) A data providing system as set forth in claim 145, wherein said management apparatus allocates identification numbers to said data providing apparatus and said data distribution apparatus in accordance with said registration and transmits to said data providing apparatus and said data distribution apparatus public key data of a route certificate authority and public key data of the management apparatus.

147. (Original) A data providing system as set forth in claim 145, wherein each of said data providing apparatus and said data distribution apparatus further registers said secret key data in said management apparatus.

148. (Original) A data providing system as set forth in claim 143, wherein said data processing apparatus has stored in it in advance secret key data generated by said management apparatus and public key data corresponding to said secret key data.

149. (Original) A data providing system as set forth in claim 148, wherein said data processing apparatus has stored in it in advance public key certificate data certifying the legitimacy of said public key data generated by said management apparatus.

150. (Currently Amended) A data providing system comprising a data providing apparatus, data distribution apparatus, data processing apparatus, and management apparatus, wherein

said data providing apparatus provides content data to said data distribution apparatus,

said data distribution apparatus distributes said provided content data to said data processing apparatus,

said data processing apparatus uses said distributed content data, and

said management apparatus manages the operation of a data providing service by said data providing apparatus, said data distribution apparatus, and said data processing apparatus, registers and serves usage control policy data indicating the handling of the related content data from said data providing apparatus, and certifies the legitimacy of said usage control policy data in response to a request from said data providing apparatus, and wherein

the transmission of data among said data providing apparatus, said data distribution apparatus, said data processing apparatus, and said management apparatus is carried out by using mutual authentication using a session key encryption method, signature creation, signature verification, and encryption of data by a common key encryption method.

151. (Currently Amended) A data providing system comprising a data providing apparatus, data distribution apparatus, data processing apparatus, and management apparatus, wherein

said data providing apparatus provides content data to said data distribution apparatus,

said data distribution apparatus distributes said provided content data to said data processing apparatus,

said data processing apparatus uses said distributed content data, and

said management apparatus manages the operation of a data providing service by said data providing apparatus, said data distribution apparatus, and said data processing apparatus, generates signature data indicating that the related data is generated by itself by using its own secret key data when each of said data providing apparatus, said data distribution apparatus, and said data processing apparatus supplies the data to another apparatus, generates and manages

public key certificate data of public key data corresponding to secret key data of said data providing apparatus, said data distribution apparatus, and said data processing apparatus when the legitimacy of the signature data corresponding to the data is verified by using the public key data of the related other apparatus when receiving the supply of the related data from the other apparatus, registers and serves usage control policy data indicating the handling of the related content data from said data providing apparatus, and certifies the legitimacy of said usage control policy data in response to a request from said data providing apparatus, and wherein

said data providing apparatus, said data distribution apparatus, and said data processing apparatus acquire said their own public key certificate data from said management apparatus before communicating with the other apparatus and transmit the related acquired public key certificate data to said other apparatus

wherein said data providing apparatus performs mutual authentication with said data processing apparatus, encrypts said module using session key data obtained by said mutual authentication, and transmits said encrypted module to said data processing apparatus.

152. (Currently Amended) A data providing system comprising a data providing apparatus, data distribution apparatus, data processing apparatus, and management apparatus, wherein

said data providing apparatus provides content data to said data distribution apparatus,

said data distribution apparatus distributes said provided content data to said data processing apparatus,

said data processing apparatus uses said distributed content data, and

said management apparatus manages the operation of a data providing service by said data providing apparatus, said data distribution apparatus, and said data processing apparatus, generates the signature data indicating that the related data is generated by itself by using its own secret key data when each of said data providing apparatus, said data distribution apparatus, and said data processing apparatus supplies data to another apparatus, generates and manages public key certificate data of public key data corresponding to secret key data of said data providing apparatus, said data distribution apparatus, and said data processing apparatus when the legitimacy of the signature data corresponding to the data is verified by using the public key data of the related other apparatus when receiving the supply of the related data from the other apparatus, registers and serves usage control policy data indicating the handling of the related content data from said data providing apparatus, and certifies the legitimacy of said usage control policy data in response to a request from said data providing apparatus,

wherein said data providing apparatus performs mutual authentication with said data processing apparatus, encrypts said module using session key data obtained by said mutual authentication, and transmits said encrypted module to said data processing apparatus, and wherein

said data providing apparatus, said data distribution apparatus, and said data processing apparatus acquire their own public key certificate data from said management apparatus before communicating with the other apparatus and transmit the related acquired public key certificate data to said other apparatus at said communication.

153. (Currently Amended) A data providing system comprising a data providing apparatus, data distribution apparatus, data processing apparatus, and management apparatus, wherein:

said data providing apparatus provides content data to said data distribution apparatus,

said data distribution apparatus distributes said provided content data to said data processing apparatus,

said data processing apparatus uses said distributed content data, and

said management apparatus manages the operation of a data providing service by said data providing apparatus, said data distribution apparatus, and said data processing apparatus, generates signature data indicating that the related data is generated by itself by using its own secret key data when each of said data providing apparatus, said data distribution apparatus, and said data processing apparatus supplies data to another apparatus, generates and manages public key certificate data of public key data corresponding to secret key data of said data providing apparatus, said data distribution apparatus, and said data processing apparatus when the legitimacy of the signature data corresponding to the data is verified by using the public key data of the related other apparatus when receiving the supply of the related data from the other apparatus, generates public key certificate revocation list for specifying public key certificate data to be invalidated among said generated public key certificate data and thereby to restrict said communication or said distribution using public key certificate data specified by said public key certificate revocation list by said data providing apparatus, said data distribution apparatus, and said data processing apparatus, registers and serves usage control policy data indicating the handling of the related content data from said data providing apparatus, and certifies the

legitimacy of said usage control policy data in response to a request from said data providing apparatus

wherein said data providing apparatus performs mutual authentication with said data processing apparatus, encrypts said module using session key data obtained by said mutual authentication, and transmits said encrypted module to said data processing apparatus.

154. (Original) A data providing system as set forth in claim 153, wherein said management apparatus generates public key certificate revocation list specifying public key certificate data corresponding to said data providing apparatus, said data distribution apparatus, and said data processing apparatus used for illegal actions.

155. (Currently Amended) A data providing system comprising a data providing apparatus, data distribution apparatus, data processing apparatus, and management apparatus, wherein:

said data providing apparatus provides content data to said data distribution apparatus,

said data distribution apparatus distributes said provided content data to said data processing apparatus,

said management apparatus manages the operation of a data providing service by said data providing apparatus, said data distribution apparatus, and said data processing apparatus, generates signature data indicating that the related data is generated by an apparatus itself by using its own secret key data when said data providing apparatus supplies data to another apparatus, generates and manages public key certificate data of public key data corresponding to secret key data of said data providing apparatus for when another apparatus verifies the legitimacy of the related signature data by using the public key data corresponding to said secret

key data, generates public key certificate revocation list for specifying public key certificate data to be invalidated among said generated public key certificate data, distributes the related public key certificate revocation list to said data processing apparatus, registers and serves usage control policy data indicating the handling of the related content data from said data providing apparatus, and certifies the legitimacy of said usage control policy data in response to a request from said data providing apparatus, and

said data processing apparatus verifies whether or not public key certificate data of said data providing apparatus providing said distributed content data is invalid based on said public key certificate revocation list distributed from said management apparatus and controls the usage of said distributed content data based on the result of the related verification

wherein said data providing apparatus performs mutual authentication with said data processing apparatus, encrypts said module using session key data obtained by said mutual authentication, and transmits said encrypted module to said data processing apparatus.

156. (Original) A data providing system as set forth in claim 155, wherein said management apparatus directly distributes said public key certificate revocation list to said data processing apparatus.

157. (Original) A data providing system as set forth in claim 155, wherein said management apparatus distributes said public key certificate revocation list to said data processing apparatus through said data distribution apparatus, by broadcasting, or by an on-demand system.

158. (Currently Amended) A data providing system comprising a data providing apparatus, data distribution apparatus, data processing apparatus, and management apparatus, wherein:

said management apparatus manages the operation of a data providing service by said data providing apparatus, said data distribution apparatus, and said data processing apparatus, generates signature data indicating that the related data is generated by an apparatus itself by using its own secret key data when said data providing apparatus supplies data to another apparatus, generates and manages public key certificate data of public key data corresponding to secret key data of said data providing apparatus for when another apparatus verifies the legitimacy of the related signature data by using the public key data corresponding to said secret key data, generates public key certificate revocation list for specifying public key certificate data to be invalidated among said generated public key certificate data, distributes the related public key certificate revocation list to said data distribution apparatus, registers and serves usage control policy data indicating the handling of the related content data from said data providing apparatus, and certifies the legitimacy of said usage control policy data in response to a request from said data providing apparatus, and

said data distribution apparatus verifies whether or not public key certificate data of said data providing apparatus providing said provided content data is invalid based on said public key certificate revocation list distributed from said management apparatus, and controls the distribution of said provided content data to said data processing apparatus based on the result of the related verification

wherein said data providing apparatus performs mutual authentication with said data processing apparatus, encrypts said module using session key data obtained by said mutual authentication, and transmits said encrypted module to said data processing apparatus.

159. (Currently Amended) A data providing system comprising a data providing apparatus, data distribution apparatus, data processing apparatus, and management apparatus, wherein:

said management apparatus manages the operation of a data providing service by said data providing apparatus, said data distribution apparatus, and said data processing apparatus, generates signature data indicating that the related data is generated by an apparatus itself by using its own secret key data when said data distribution apparatus supplies data to another apparatus, generates and manages public key certificate data of public key data corresponding to secret key data of said data distribution apparatus for when another apparatus verifies the legitimacy of the related signature data by using the public key data corresponding to said secret key data, generates public key certificate revocation list for specifying public key certificate data to be invalidated among said generated public key certificate data, distributes the related public key certificate revocation list to said data providing apparatus, registers and serves usage control policy data indicating the handling of the related content data from said data providing apparatus, and certifies the legitimacy of said usage control policy data in response to a request from said data providing apparatus,

said data providing apparatus verifies whether or not public key certificate data of the data distribution apparatus of the destination of provision of the content data is invalid and

controls the provision of said content data to said data distribution apparatus based on the result of the related verification,

said data distribution apparatus distributes said provided content data to said data processing apparatus, and

said data processing apparatus uses said distributed content data

wherein said data providing apparatus performs mutual authentication with said data processing apparatus, encrypts said module using session key data obtained by said mutual authentication, and transmits said encrypted module to said data processing apparatus.

160. (Currently Amended) A data providing system comprising a data providing apparatus, data distribution apparatus, data processing apparatus, and management apparatus, wherein:

said management apparatus manages the operation of a data providing service by said data providing apparatus, said data distribution apparatus, and said data processing apparatus, generates signature data indicating that the related data is generated by an apparatus itself by using its own secret key data when said data distribution apparatus supplies data to another apparatus, generates and manages public key certificate data of public key data corresponding to secret key data of said data distribution apparatus for when another apparatus verifies the legitimacy of the related signature data by using the public key data corresponding to said secret key data, generates public key certificate revocation list for specifying public key certificate data to be invalidated among said generated public key certificate data, distributes the related public key certificate revocation list to said data distribution apparatus, registers and serves usage control policy data indicating the handling of the related content data from said data providing

apparatus, and certifies the legitimacy of said usage control policy data in response to a request from said data providing apparatus,

said data providing apparatus provides content data to said data distribution apparatus,

said data distribution apparatus distributes said provided content data and said distributed public key certificate revocation list to said data processing apparatus, and

said data processing apparatus verifies whether or not public key certificate data of said data distribution apparatus distributing said distributed content data is invalid based on said distributed public key certificate revocation list and controls the usage of said distributed content data based on the result of the related verification

wherein said data providing apparatus performs mutual authentication with said data processing apparatus, encrypts said module using session key data obtained by said mutual authentication, and transmits said encrypted module to said data processing apparatus.

161. (Original) A data providing system as set forth in claim 160, wherein said data distribution apparatus has a configuration which makes it difficult to tamper with said public key certificate revocation list distributed from said management apparatus.

162. (Original) A data providing system as set forth in claim 160, wherein

said management apparatus encrypts said public key certificate revocation list using distribution key data and distributes it to said data distribution apparatus and distributes said distribution key data to said data processing apparatus and

said data processing apparatus decrypts said distributed public key certificate revocation list using said distribution key data.

163. (Original) A data providing system as set forth in claim 160, wherein said data distribution apparatus distributes said public key certificate revocation list to said data processing apparatus by broadcasting or by an on-demand system.

164. (Currently Amended) A data providing system comprising a data providing apparatus, data distribution apparatus, data processing apparatus, and management apparatus, wherein:

said management apparatus manages the operation of a data providing service by said data providing apparatus, said data distribution apparatus, and said data processing apparatus, generates signature data indicating that the related data is generated by an apparatus itself by using its own secret key data when said data distribution apparatus supplies data to another apparatus, generates and manages public key certificate data of public key data corresponding to secret key data of said data distribution apparatus for when another apparatus verifies the legitimacy of the related signature data by using public key data corresponding to said secret key data, generates public key certificate revocation list for specifying public key certificate data to be invalidated among said generated public key certificate data, distributes the related public key certificate revocation list to said data processing apparatus, registers and serves usage control policy data indicating the handling of the related content data from said data providing apparatus, and certifies the legitimacy of said usage control policy data in response to a request from said data providing apparatus,

said data providing apparatus provides content data to said data distribution apparatus,

said data distribution apparatus distributes said provided content data to said data processing apparatus, and

said data processing apparatus verifies whether or not public key certificate data of said data distribution apparatus distributing said distributed content data is invalid based on said distributed public key certificate revocation list and controls the usage of said distributed content data based on the result of the related verification

wherein said data providing apparatus performs mutual authentication with said data processing apparatus, encrypts said module using session key data obtained by said mutual authentication, and transmits said encrypted module to said data processing apparatus.

165. (Currently Amended) A data providing system comprising a data providing apparatus, data distribution apparatus, data processing apparatus, and management apparatus, wherein:

said management apparatus manages the operation of a data providing service by said data providing apparatus, said data distribution apparatus, and said data processing apparatus, generates signature data indicating that the related data is generated by an apparatus itself by using its own secret key data when said data distribution apparatus supplies data to another apparatus, generates and manages public key certificate data of public key data corresponding to secret key data of said data distribution apparatus for when another apparatus verifies the legitimacy of the related signature data by using public key data corresponding to said secret key data, generates public key certificate revocation list for specifying public key certificate data to be invalidated among said generated public key certificate data, distributes the related public key certificate revocation list to said data providing apparatus, registers and serves usage control policy data indicating the handling of the related content data from said data providing apparatus,

and certifies the legitimacy of said usage control policy data in response to a request from said data providing apparatus,

said data providing apparatus provides content data and said public key certificate revocation list to said data distribution apparatus,

said data distribution apparatus distributes said provided content data and public key certificate revocation list to said data processing apparatus

said data providing apparatus performs mutual authentication with said data processing apparatus, encrypts said module using session key data obtained by said mutual authentication, and transmits said encrypted module to said data processing apparatus, and

said data processing apparatus verifies whether or not public key certificate data of said data distribution apparatus distributing said distributed content data is invalid based on said distributed public key certificate revocation list and controls the usage of said distributed content data based on the result of the related verification.

166. (Currently Amended) A data providing system comprising a data providing apparatus, data distribution apparatus, a plurality of data processing apparatuses, and a management apparatus, wherein:

said management apparatus manages the operation of a data providing service by said data providing apparatus, said data distribution apparatus, and said data processing apparatuses, generates signature data indicating that the related data is generated by an apparatus itself by using its own secret key data when a data processing apparatus supplies data to another apparatus, generates and manages public key certificate data of public key data corresponding to secret key data of said data processing apparatuses for when another apparatus verifies the

legitimacy of the related signature data by using the public key data corresponding to said secret key data, generates public key certificate revocation list for specifying public key certificate data to be invalidated among said generated public key certificate data, distributes the related public key certificate revocation list to said data providing apparatus, registers and serves usage control policy data indicating the handling of the related content data from said data providing apparatus, and certifies the legitimacy of said usage control policy data in response to a request from said data providing apparatus,

said data providing apparatus provides content data and said public key certificate revocation list to said data distribution apparatus,

said data providing apparatus performs mutual authentication with said data processing apparatus, encrypts said module using session key data obtained by said mutual authentication, and transmits said encrypted module to said data processing apparatus,

said data distribution apparatus distributes said provided content data and public key certificate revocation list to said data processing apparatuses, and

said data processing apparatuses verify whether or not public key certificate data of said other data processing apparatuses are invalid based on the public key certificate revocation list distributed from said data distribution apparatus and control the communication with other data processing apparatuses based on the result of the related verification.

167. (Original) A data providing system as set forth in claim 166, wherein said data distribution apparatus has a configuration which makes it difficult to tamper with said public key certificate revocation list distributed from said management apparatus.

168. (Original) A data providing system as set forth in claim 166, wherein

said management apparatus encrypts said public key certificate revocation list using distribution key data and distributes it to said data distribution apparatus and distributes said distribution key data to said data processing apparatus and

said data processing apparatus decrypts said distributed public key certificate revocation list using said distribution key data.

169. (Currently Amended) A data providing system comprising a data providing apparatus, data distribution apparatus, a plurality of data processing apparatuses, and a management apparatus, wherein:

said management apparatus manages the operation of a data providing service by said data providing apparatus, said data distribution apparatus, and said data processing apparatuses, generates signature data indicating that the related data is generated by an apparatus itself by using its own secret key data when a data processing apparatus supplies data to another apparatus, generates and manages public key certificate data of public key data corresponding to secret key data of said data processing apparatuses for when another apparatus verifies the legitimacy of the related signature data by using the public key data corresponding to said secret key data, generates public key certificate revocation list for specifying public key certificate data to be invalidated among said generated public key certificate data, distributes the related public key certificate revocation list to said data providing apparatus, registers and serves usage control policy data indicating the handling of the related content data from said data providing apparatus, and certifies the legitimacy of said usage control policy data in response to a request from said data providing apparatus,

said data providing apparatus provides content data to said data distribution apparatus,

said data providing apparatus performs mutual authentication with said data processing apparatus, encrypts said module using session key data obtained by said mutual authentication, and transmits said encrypted module to said data processing apparatus,

said data distribution apparatus distributes said provided content data and said distributed public key certificate revocation list to said data processing apparatuses, and

said data processing apparatuses verify whether or not public key certificate data of other data processing apparatuses are invalid based on the public key certificate revocation list distributed from said data distribution apparatus, and control the communication with other data processing apparatuses based on the result of the related verification.

170. (Original) A data providing system as set forth in claim 169, wherein said data distribution apparatus has a configuration which makes it difficult to tamper with said public key certificate revocation list distributed from said management apparatus.

171. (Original) A data providing system as set forth in claim 169, wherein

said management apparatus encrypts said public key certificate revocation list using distribution key data and distributes it to said data distribution apparatus and distributes said distribution key data to said data processing apparatus and

said data processing apparatus decrypts said distributed public key certificate revocation list using said distribution key data.

172. (Currently Amended) A data providing system comprising a data providing apparatus, data distribution apparatus, a plurality of data processing apparatuses, and a management apparatus, wherein:

a data processing apparatus supplies registration data, indicating an already registered data processing apparatus connected in a predetermined network to which is connected, to said management apparatus, refers to a revocation flag in registration data supplied from said management apparatus and restricts communication with another data processing apparatus having public key certificate data indicated as invalid by the revocation flag,

said management apparatus manages the operation of a data providing service by said data providing apparatus, said data distribution apparatus, and said data processing apparatuses, generates and manages public key certificate data of public key data corresponding to secret key data for when a data processing apparatus generates signature data indicating legitimacy of data using its own secret key data when supplying data to another apparatus, generates public key certificate revocation list for specifying public key certificate data to be invalidated among said generated public key certificate data, stores the related public key certificate revocation list, generates new registration data by setting said revocation flag in said registration data supplied from data processing apparatuses based on the related public key certificate revocation list, distributes the related generated registration data to said data processing apparatuses, registers and serves usage control policy data indicating the handling of the related content data from said data providing apparatus, and certifies the legitimacy of said usage control policy data in response to a request from said data providing apparatus,

said data providing apparatus provides content data to said data distribution apparatus,

said data providing apparatus performs mutual authentication with said data processing apparatus, encrypts said module using session key data obtained by said mutual authentication, and transmits said encrypted module to said data processing apparatus, and

said data distribution apparatus distributes said provided content data to said data processing apparatuses.

173. (Currently Amended) A data providing system comprising a data providing apparatus, data distribution apparatus, a plurality of data processing apparatuses, and a management apparatus, wherein:

said management apparatus manages the operation of a data providing service by said data providing apparatus, said data distribution apparatus, and said data processing apparatuses, generates and manages public key certificate data of public key data corresponding to said secret key data for when a data processing apparatus generates signature data indicating the legitimacy of data by using its own secret key data when supplying the related data to another apparatus, generates public key certificate revocation list for specifying public key certificate data to be invalidated among said generated public key certificate data, distributes the related public key certificate revocation list to said data providing apparatus, registers and serves usage control policy data indicating the handling of the related content data from said data providing apparatus, and certifies the legitimacy of said usage control policy data in response to a request from said data providing apparatus,

said data providing apparatus provides content data and said public key certificate revocation list to said data distribution apparatus,

said data distribution apparatus distributes said provided content data and said public key certificate revocation list to said data processing apparatuses,

said data providing apparatus performs mutual authentication with said data processing apparatus, encrypts said module using session key data obtained by said mutual authentication, and transmits said encrypted module to said data processing apparatus, and

a data processing apparatus sets a revocation flag in registration data indicating an already registered data processing apparatus connected in a predetermined network to which it is connected based on said distributed public key certificate revocation list and restricts communication with another data processing apparatus having public key certificate data indicated as invalid by the related revocation flag.

174. (Currently Amended) A data providing system comprising a data providing apparatus, data distribution apparatus, a plurality of data processing apparatuses, and a management apparatus, wherein:

said management apparatus manages the operation of a data providing service by said data providing apparatus, said data distribution apparatus, and said data processing apparatuses, generates and manages public key certificate data of public key data corresponding to secret key data for when a data processing apparatus generates signature data indicating the legitimacy of the data by using its own secret key data when supplying the related data to another apparatus, generates public key certificate revocation list for specifying public key certificate data to be invalidated among said generated public key certificate data, distributes the related public key certificate revocation list to said data distribution apparatus, registers and serves usage control policy data indicating the handling of the related content data from said data providing apparatus,

and certifies the legitimacy of said usage control policy data in response to a request from said data providing apparatus,

said data providing apparatus provides content data to said data distribution apparatus,

said data distribution apparatus distributes said provided content data and said public key certificate revocation list to said data processing apparatuses,

said data providing apparatus performs mutual authentication with said data processing apparatus, encrypts said module using session key data obtained by said mutual authentication, and transmits said encrypted module to said data processing apparatus, and

a data processing apparatus sets a revocation flag in registration data indicating an already registered data processing apparatus connected in a predetermined network to which it is connected based on said distributed public key certificate revocation list and restricts communication with another data processing apparatus having public key certificate data indicated as invalid by the related revocation flag.

175. (Currently Amended) A data providing system comprising:

a data providing apparatus that provides content data and usage control policy data indicating the handling of the related content data to said data distribution apparatus,

a data distribution apparatus that distributes said provided content data and said usage control policy data to said data processing apparatus,

a data processing apparatus that has a first module for communicating with said data distribution apparatus and a second module for determining at least one of a purchase mode and usage mode of said distributed content data based on said distributed usage control policy data

and transmitting log data indicating the log of the related determined purchase mode and usage mode to said management apparatus,

a management apparatus that manages the data providing apparatus, data distribution apparatus, and data processing apparatus and

has a settlement function for performing profit distribution processing for distributing the profit obtained accompanied with said data processing apparatus receiving distribution of said content data and purchasing and using said content data to related parties of said data providing apparatus and said data distribution apparatus based on said log data received from said second module and performing settlement based on the result of the related profit distribution processing and a right management function for registering said usage control policy data,

wherein said data providing apparatus sends said usage control policy data and requests to said management apparatus to certify legitimacy of said usage control policy data, and wherein said management apparatus registers and serves said usage control policy data from said data providing apparatus, and certifies the legitimacy of said usage control policy data in response to a request from said data providing apparatus

wherein said data providing apparatus performs mutual authentication with said data processing apparatus, encrypts said module using session key data obtained by said mutual authentication, and transmits said encrypted module to said data processing apparatus.

176. (Original) A data providing system as set forth in claim 175, wherein said management apparatus has

a first management apparatus having a settlement function and

a second management apparatus having a right management function.

177. (Original) A data providing system as set forth in claim 175, wherein said settlement is electronic settlement.

178. (Currently Amended) A data providing system comprising:

a data providing apparatus that provides content data and usage control policy data indicating the handling of the related content data to said data distribution apparatus,

a data distribution apparatus that has a charging function for performing settlement processing by using settlement claim data distributed from said management apparatus and distributes said provided content data and said usage control policy data to said data processing apparatus,

a data processing apparatus that has a first module for communicating with said data distribution apparatus and a second module for determining at least one of a purchase mode and usage mode of said distributed content data based on said distributed usage control policy data and transmitting log data indicating the log of the related determined purchase mode and usage mode to said management apparatus,

a management apparatus that manages the data providing apparatus, data distribution apparatus, and data processing apparatus and

has a settlement claim data creation function for performing profit distribution processing for distributing the profit obtained accompanied with said data processing apparatus receiving distribution of said content data and purchasing and using said content data to related parties of said data providing apparatus and said data distribution apparatus based on said log data received from said second module, creating settlement claim data used when performing settlement based on the result of the related profit distribution processing, and supplying the same to said data

distribution apparatus and a right management function for registering said usage control policy data,

wherein said data providing apparatus performs mutual authentication with said data processing apparatus, encrypts said module using session key data obtained by said mutual authentication, and transmits said encrypted module to said data processing apparatus,

wherein said data providing apparatus sends said usage control policy data and requests to said management apparatus to certify legitimacy of said usage control policy data, and wherein said management apparatus registers and serves said usage control policy data from said data providing apparatus, and certifies the legitimacy of said usage control policy data in response to a request from said data providing apparatus.

179. (Currently Amended) A data providing system comprising:

a data providing apparatus that has a charging function for performing settlement processing by using settlement claim data distributed from said management apparatus and provides content data and usage control policy data indicating the handling of the related content data to said data distribution apparatus,

a data distribution apparatus that distributes said provided content data and said usage control policy data to said data processing apparatus,

a data processing apparatus that has a first module for communicating with said data distribution apparatus and a second module for determining at least one of a purchase mode and usage mode of said distributed content data based on said distributed usage control policy data and transmitting log data indicating the log of the related determined purchase mode and usage mode to said management apparatus,

a management apparatus that manages the data providing apparatus, data distribution apparatus, and data processing apparatus and

has a settlement claim data creation function for performing profit distribution processing for distributing the profit obtained accompanied with said data processing apparatus receiving said distribution of said content data and purchasing and using said content data to related parties of said data providing apparatus and said data distribution apparatus based on said log data received from said second module, creating settlement claim data used when performing settlement based on the result of the related profit distribution processing, and distributing the same to said data providing apparatus and a right management function for registering said usage control policy data,

wherein said data providing apparatus performs mutual authentication with said data processing apparatus, encrypts said module using session key data obtained by said mutual authentication, and transmits said encrypted module to said data processing apparatus,

wherein said data providing apparatus sends said usage control policy data and requests to said management apparatus to certify legitimacy of said usage control policy data, and wherein said management apparatus registers and serves said usage control policy data from said data providing apparatus, and certifies the legitimacy of said usage control policy data in response to a request from said data providing apparatus.

180. (Currently Amended) A data providing method using a data providing apparatus, data processing apparatus, and management apparatus comprising the steps of

distributing content data and usage control policy data indicating the handling of the related content data from said data providing apparatus to said data processing apparatus,

determining at least one of the purchase mode and the usage mode of said distributed content data based on said distributed usage control policy data and transmitting log data indicating the log of at least one of the related determined purchase mode and usage mode to said management apparatus at said data processing apparatus,

registering and serving said usage control policy data from said data providing apparatus,

certifies the legitimacy of said usage control policy data in response to a request from said data providing apparatus, and

performing profit distribution processing for distributing the profit obtained accompanied with said purchase and said usage of said content data in said data processing apparatus to related parties of said data providing apparatus based on said received log data at said management apparatus.

181. (Currently Amended) A data providing method using a data providing apparatus, data distribution apparatus, data processing apparatus, and management apparatus comprising the steps of:

providing content data and usage control policy data indicating the handling of the related content data from said data providing apparatus to said data distribution apparatus,

performing mutual authentication with said data processing apparatus, encrypting said module using session key data obtained by said mutual authentication, and transmitting said encrypted module to said data processing apparatus

distributing said provided content data and said usage control policy data from said data distribution apparatus to said data processing apparatus,

determining at least one of the purchase mode and the usage mode of said distributed content data based on said distributed usage control policy data and transmitting log data indicating the log of the related determined purchase mode and usage mode to said management apparatus at said data processing apparatus,

registering and serving said usage control policy data from said data providing apparatus,

certifies the legitimacy of said usage control policy data in response to a request from said data providing apparatus, and

performing profit distribution processing for distributing the profit obtained accompanied with said data processing apparatus receiving said distribution of said content data and purchasing and using said content data to related parties of said data providing apparatus and said data distribution apparatus based on said log data received from said second module at said management apparatus.

182. (Currently Amended) A data providing method using a data providing apparatus, data distribution apparatus, data processing apparatus, and management apparatus comprising the steps of:

providing content data and usage control policy data indicating the handling of the related content data from said data providing apparatus to said data distribution apparatus,

performing mutual authentication with said data processing apparatus, encrypting said module using session key data obtained by said mutual authentication, and transmitting said encrypted module to said data processing apparatus,

distributing said content data and said usage control policy data provided from said data distribution apparatus to said data processing apparatus to said data processing apparatus,

generating data distribution apparatus use purchase log data indicating the log of the purchase of said content data distributed from said data distribution apparatus and transmitting the same to said data distribution apparatus, determining at least one of a purchase mode and usage mode of said distributed content data based on said distributed usage control policy data, and transmitting management apparatus use log data indicating the log of the related determined purchase mode and usage mode to said management apparatus at said data processing apparatus,

distributing the profit obtained accompanied with said purchase and said usage of said content data in said data processing apparatus to related parties of said data providing apparatus and said data distribution apparatus based on said management apparatus use log data at said management apparatus,

registering and serving said usage control policy data from said data providing apparatus,

certifies the legitimacy of said usage control policy data in response to a request from said data providing apparatus, and

performing charging processing concerning the distribution of said content data based on the data distribution apparatus use purchase log data received from said data processing apparatus at said data distribution apparatus.

183. (Currently Amended) A data providing method using a data providing apparatus, data distribution apparatus, data processing apparatus, and management apparatus to provide content data, wherein

said data providing apparatus provides content data to said data distribution apparatus,

said data distribution apparatus distributes said provided content data to said data processing apparatus,

said data providing apparatus performs mutual authentication with said data processing apparatus, encrypts said module using session key data obtained by said mutual authentication, and transmits said encrypted module to said data processing apparatus, and

said data processing apparatus manages the operation of a data provision service by said data providing apparatus, data distribution apparatus, and data processing apparatus, and

said management apparatus manages operation of a data providing service by said data providing apparatus, said data distribution apparatus, and said data processing apparatus, registers and serves usage control policy data indicating the handling of the related content data from said data providing apparatus, and certifies the legitimacy of said usage control policy data in response to a request from said data providing apparatus, and wherein

the transmission of data among said data providing apparatus, said data distribution apparatus, said data processing apparatus, and said management apparatus is carried out by using mutual authentication using a public key encryption method, signature creation, signature verification, and encryption of data by a common key encryption method.

184. (Currently Amended) A data providing method using a data providing apparatus, data distribution apparatus, data processing apparatus, and management apparatus to provide content data, wherein

said data providing apparatus provides content data to said data distribution apparatus,

said data providing apparatus performs mutual authentication with said data processing apparatus, encrypts said module using session key data obtained by said mutual authentication, and transmits said encrypted module to said data processing apparatus,

said data distribution apparatus distributes said provided content data to said data processing apparatus,

said data processing apparatus uses said distributed content data, and

said management apparatus manages the operation of a data providing service by said data providing apparatus, said data distribution apparatus, and said data processing apparatus, generates signature data indicating that the related data is generated by itself by using its own secret key data when each of said data providing apparatus, said data distribution apparatus, and said data processing apparatus supplies the data to another apparatus, generates and manages public key certificate data of public key data corresponding to secret key data of said data providing apparatus, said data distribution apparatus, and said data processing apparatus when the legitimacy of the signature data corresponding to the data is verified by using the public key data of the related other apparatus when receiving the supply of the related data from the other apparatus, registers and serves usage control policy data indicating the handling of the related content data from said data providing apparatus, and certifies the legitimacy of said usage control policy data in response to a request from said data providing apparatus, and wherein

said data providing apparatus, said data distribution apparatus, and said data processing apparatus acquire said their own public key certificate data from said management apparatus before communicating with the other apparatus and transmit the related acquired public key certificate data to said other apparatus.

185. (Currently Amended) A data providing method using a data providing apparatus, data distribution apparatus, data processing apparatus, and management apparatus to provide content data, wherein

said data providing apparatus provides content data to said data distribution apparatus,

said data distribution apparatus distributes said provided content data to said data processing apparatus,

said data providing apparatus performs mutual authentication with said data processing apparatus, encrypts said module using session key data obtained by said mutual authentication, and transmits said encrypted module to said data processing apparatus,

said data processing apparatus uses said distributed content data, and

said management apparatus manages the operation of a data providing service by said data providing apparatus, said data distribution apparatus, and said data processing apparatus, generates the signature data indicating that the related data is generated by itself by using its own secret key data when each of said data providing apparatus, said data distribution apparatus, and said data processing apparatus supplies data to another apparatus, generates and manages public key certificate data of public key data corresponding to secret key data of said data providing apparatus, said data distribution apparatus, and said data processing apparatus when the legitimacy of the signature data corresponding to the data is verified by using the public key data of the related other apparatus when receiving the supply of the related data from the other apparatus, registers and serves usage control policy data indicating the handling of the related content data from said data providing apparatus, and certifies the legitimacy of said usage control policy data in response to a request from said data providing apparatus, and wherein

said data providing apparatus, said data distribution apparatus, and said data processing apparatus acquire their own public key certificate data from said management apparatus when

communicating with the other apparatus and transmit the related acquired public key certificate data to said other apparatus at said communication.

186. (Currently Amended) A data providing method using a data providing apparatus, data distribution apparatus, data processing apparatus, and management apparatus to provide content data, wherein:

said data providing apparatus provides content data to said data distribution apparatus,

said data distribution apparatus distributes said provided content data to said data processing apparatus,

said data processing apparatus uses said distributed content data,

said data providing apparatus performs mutual authentication with said data processing apparatus, encrypts said module using session key data obtained by said mutual authentication, and transmits said encrypted module to said data processing apparatus, and

said management apparatus manages the operation of a data providing service by said data providing apparatus, said data distribution apparatus, and said data processing apparatus, generates signature data indicating that the related data is generated by itself by using its own secret key data when each of said data providing apparatus, said data distribution apparatus, and said data processing apparatus supplies data to another apparatus, generates and manages public key certificate data of public key data corresponding to secret key data of said data providing apparatus, said data distribution apparatus, and said data processing apparatus when the legitimacy of the signature data corresponding to the data is verified by using the public key data of the related other apparatus when receiving the supply of the related data from the other apparatus, generates public key certificate revocation list for specifying public key certificate

data to be invalidated among said generated public key certificate data and thereby to restrict said communication or said distribution using public key certificate data specified by said public key certificate revocation list by said data providing apparatus, said data distribution apparatus, and said data processing apparatus, registers and serves usage control policy data indicating the handling of the related content data from said data providing apparatus, and certifies the legitimacy of said usage control policy data in response to a request from said data providing apparatus.

187. (Original) A data providing method as set forth in claim 186, wherein said management apparatus generates public key certificate revocation list specifying public key certificate data corresponding to said data providing apparatus, said data distribution apparatus, and said data processing apparatus used for illegal actions.

188. (Currently Amended) A data providing method using a data providing apparatus, data distribution apparatus, data processing apparatus, and management apparatus to provide content data, wherein:

said data providing apparatus provides content data to said data distribution apparatus,

said data distribution apparatus distributes said provided content data to said data processing apparatus,

said data providing apparatus performs mutual authentication with said data processing apparatus, encrypts said module using session key data obtained by said mutual authentication, and transmits said encrypted module to said data processing apparatus,

said management apparatus manages the operation of a data providing service by said data providing apparatus, said data distribution apparatus, and said data processing apparatus,

generates signature data indicating that the related data is generated by an apparatus itself by using its own secret key data when said data providing apparatus supplies data to another apparatus, generates and manages public key certificate data of public key data corresponding to secret key data of said data providing apparatus for when another apparatus verifies the legitimacy of the related signature data by using the public key data corresponding to said secret key data, generates public key certificate revocation list for specifying public key certificate data to be invalidated among said generated public key certificate data, distributes the related public key certificate revocation list to said data processing apparatus, registers and serves usage control policy data indicating the handling of the related content data from said data providing apparatus, and certifies the legitimacy of said usage control policy data in response to a request from said data providing apparatus, and

said data processing apparatus verifies whether or not public key certificate data of said data providing apparatus providing said distributed content data is invalid based on said public key certificate revocation list distributed from said management apparatus and controls the usage of said distributed content data based on the result of the related verification.

189. (Original) A data providing method as set forth in claim 188, wherein said management apparatus directly distributes said public key certificate revocation list to said data processing apparatus.

190. (Original) A data providing method as set forth in claim 188, wherein said management apparatus distributes said public key certificate revocation list to said data processing apparatus through said data distribution apparatus, by broadcasting, or by an on-demand system.

191. (Currently Amended) A data providing method using a data providing apparatus, data distribution apparatus, data processing apparatus, and management apparatus to provide content data, wherein:

said management apparatus manages the operation of a data providing service by said data providing apparatus, said data distribution apparatus, and said data processing apparatus, generates signature data indicating that the related data is generated by an apparatus itself by using its own secret key data when said data providing apparatus supplies data to another apparatus, generates and manages public key certificate data of public key data corresponding to secret key data of said data providing apparatus for when another apparatus verifies the legitimacy of the related signature data by using the public key data corresponding to said secret key data, generates public key certificate revocation list for specifying public key certificate data to be invalidated among said generated public key certificate data, distributes the related public key certificate revocation list to said data distribution apparatus, registers and serves usage control policy data indicating the handling of the related content data from said data providing apparatus, and certifies the legitimacy of said usage control policy data in response to a request from said data providing apparatus,

said data providing apparatus performs mutual authentication with said data processing apparatus, encrypts said module using session key data obtained by said mutual authentication, and transmits said encrypted module to said data processing apparatus, and

said data distribution apparatus verifies whether or not public key certificate data of said data providing apparatus providing said provided content data is invalid based on said public key certificate revocation list distributed from said management apparatus, and controls the

distribution of said provided content data to said data processing apparatus based on the result of the related verification.

192. (Currently Amended) A data providing method using a data providing apparatus, data distribution apparatus, data processing apparatus, and management apparatus to provide content data, wherein:

said management apparatus manages the operation of a data providing service by said data providing apparatus, said data distribution apparatus, and said data processing apparatus, generates signature data indicating that the related data is generated by an apparatus itself by using its own secret key data when said data distribution apparatus supplies data to another apparatus, generates and manages public key certificate data of public key data corresponding to secret key data of said data distribution apparatus for when another apparatus verifies the legitimacy of the related signature data by using the public key data corresponding to said secret key data, generates public key certificate revocation list for specifying public key certificate data to be invalidated among said generated public key certificate data, distributes the related public key certificate revocation list to said data providing apparatus, registers and serves usage control policy data indicating the handling of the related content data from said data providing apparatus, and certifies the legitimacy of said usage control policy data in response to a request from said data providing apparatus,

wherein said data providing apparatus performs mutual authentication with said data processing apparatus, encrypts said module using session key data obtained by said mutual authentication, and transmits said encrypted module to said data processing apparatus,

said data providing apparatus verifies whether or not public key certificate data of the data distribution apparatus of the destination of provision of the content data is invalid and controls the provision of said content data to said data distribution apparatus based on the result of the related verification,

said data distribution apparatus distributes said provided content data to said data processing apparatus, and

said data processing apparatus uses said distributed content data.

193. (Currently Amended) A data providing method using a data providing apparatus, data distribution apparatus, data processing apparatus, and management apparatus to provide content data, wherein:

said management apparatus manages the operation of a data providing service by said data providing apparatus, said data distribution apparatus, and said data processing apparatus, generates signature data indicating that the related data is generated by an apparatus itself by using its own secret key data when said data distribution apparatus supplies data to another apparatus, generates and manages public key certificate data of public key data corresponding to secret key data of said data distribution apparatus for when another apparatus verifies the legitimacy of the related signature data by using the public key data corresponding to said secret key data, generates public key certificate revocation list for specifying public key certificate data to be invalidated among said generated public key certificate data, distributes the related public key certificate revocation list to said data distribution apparatus, registers and serves usage control policy data indicating the handling of the related content data from said data providing

apparatus, and certifies the legitimacy of said usage control policy data in response to a request from said data providing apparatus,

said data providing apparatus provides content data to said data distribution apparatus,

said data providing apparatus performs mutual authentication with said data processing apparatus, encrypts said module using session key data obtained by said mutual authentication, and transmits said encrypted module to said data processing apparatus,

said data distribution apparatus distributes said provided content data and said distributed public key certificate revocation list to said data processing apparatus, and

said data processing apparatus verifies whether or not public key certificate data of said data distribution apparatus distributing said distributed content data is invalid based on said distributed public key certificate revocation list and controls the usage of said distributed content data based on the result of the related verification.

194. (Original) A data providing method as set forth in claim 193, wherein said data distribution apparatus has a configuration which makes it difficult to tamper with said public key certificate revocation list distributed from said management apparatus.

195. (Original) A data providing method as set forth in claim 193, wherein

said management apparatus encrypts said public key certificate revocation list using distribution key data and distributes it to said data distribution apparatus and distributes said distribution key data to said data processing apparatus and

said data processing apparatus decrypts said distributed public key certificate revocation list using said distribution key data.

196. (Original) A data providing method as set forth in claim 160, wherein said data distribution apparatus distributes said public key certificate revocation list to said data processing apparatus by broadcasting or by an on-demand system.

197. (Currently Amended) A data providing method using a data providing apparatus, data distribution apparatus, data processing apparatus, and management apparatus to provide content data, wherein:

said management apparatus manages the operation of a data providing service by said data providing apparatus, said data distribution apparatus, and said data processing apparatus, generates signature data indicating that the related data is generated by an apparatus itself by using its own secret key data when said data distribution apparatus supplies data to another apparatus, generates and manages public key certificate data of public key data corresponding to secret key data of said data distribution apparatus for when another apparatus verifies the legitimacy of the related signature data by using public key data corresponding to said secret key data, generates public key certificate revocation list for specifying public key certificate data to be invalidated among said generated public key certificate data, distributes the related public key certificate revocation list to said data processing apparatus, registers and serves usage control policy data indicating the handling of the related content data from said data providing apparatus, and certifies the legitimacy of said usage control policy data in response to a request from said data providing apparatus,

said data providing apparatus provides content data to said data distribution apparatus,

said data providing apparatus performs mutual authentication with said data processing apparatus, encrypts said module using session key data obtained by said mutual authentication, and transmits said encrypted module to said data processing apparatus,

said data distribution apparatus distributes said provided content data to said data processing apparatus, and

said data processing apparatus verifies whether or not public key certificate data of said data distribution apparatus distributing said distributed content data is invalid based on said distributed public key certificate revocation list and controls the usage of said distributed content data based on the result of the related verification.

198. (Currently Amended) A data providing method using a data providing apparatus, data distribution apparatus, data processing apparatus, and management apparatus to provide content data, wherein:

said management apparatus manages the operation of a data providing service by said data providing apparatus, said data distribution apparatus, and said data processing apparatus, generates signature data indicating that the related data is generated by an apparatus itself by using its own secret key data when said data distribution apparatus supplies data to another apparatus, generates and manages public key certificate data of public key data corresponding to secret key data of said data distribution apparatus for when another apparatus verifies the legitimacy of the related signature data by using public key data corresponding to said secret key data, generates public key certificate revocation list for specifying public key certificate data to be invalidated among said generated public key certificate data, distributes the related public key certificate revocation list to said data providing apparatus, registers and serves usage control

policy data indicating the handling of the related content data from said data providing apparatus, and certifies the legitimacy of said usage control policy data in response to a request from said data providing apparatus,

said data providing apparatus performs mutual authentication with said data processing apparatus, encrypts said module using session key data obtained by said mutual authentication, and transmits said encrypted module to said data processing apparatus,

said data providing apparatus provides content data and said public key certificate revocation list to said data distribution apparatus,

said data distribution apparatus distributes said provided content data and public key certificate revocation list to said data processing apparatus, and

said data processing apparatus verifies whether or not public key certificate data of said data distribution apparatus distributing said distributed content data is invalid based on said distributed public key certificate revocation list and controls the usage of said distributed content data based on the result of the related verification.

199. (Currently Amended) A data providing method using a data providing apparatus, data distribution apparatus, a plurality of data processing apparatuses, and a management apparatus to provide content data, wherein:

said management apparatus manages the operation of a data providing service by said data providing apparatus, said data distribution apparatus, and said data processing apparatuses, generates signature data indicating that the related data is generated by an apparatus itself by using its own secret key data when a data processing apparatus supplies data to another apparatus, generates and manages public key certificate data of public key data corresponding to

secret key data of said data processing apparatuses for when another apparatus verifies the legitimacy of the related signature data by using the public key data corresponding to said secret key data, generates public key certificate revocation list for specifying public key certificate data to be invalidated among said generated public key certificate data, distributes the related public key certificate revocation list to said data providing apparatus, registers and serves usage control policy data indicating the handling of the related content data from said data providing apparatus, and certifies the legitimacy of said usage control policy data in response to a request from said data providing apparatus,

said data providing apparatus performs mutual authentication with said data processing apparatus, encrypts said module using session key data obtained by said mutual authentication, and transmits said encrypted module to said data processing apparatus,

said data providing apparatus provides content data and said public key certificate revocation list to said data distribution apparatus,

said data distribution apparatus distributes said provided content data and public key certificate revocation list to said data processing apparatuses, and

said data processing apparatuses verify whether or not public key certificate data of said other data processing apparatuses are invalid based on the public key certificate revocation list distributed from said data distribution apparatus and control the communication with other data processing apparatuses based on the result of the related verification.

200. (Original) A data providing method as set forth in claim 199, wherein said data distribution apparatus has a configuration which makes it difficult to tamper with said public key certificate revocation list distributed from said management apparatus.

201. (Original) A data providing method as set forth in claim 199, wherein

said management apparatus encrypts said public key certificate revocation list using distribution key data and distributes it to said data distribution apparatus and distributes said distribution key data to said data processing apparatus and

said data processing apparatus decrypts said distributed public key certificate revocation list using said distribution key data.

202. (Currently Amended) A data providing method using a data providing apparatus, data distribution apparatus, a plurality of data processing apparatuses, and a management apparatus to provide content data, wherein:

said management apparatus manages the operation of a data providing service by said data providing apparatus, said data distribution apparatus, and said data processing apparatuses, generates signature data indicating that the related data is generated by an apparatus itself by using its own secret key data when a data processing apparatus supplies data to another apparatus, generates and manages public key certificate data of public key data corresponding to secret key data of said data processing apparatuses for when another apparatus verifies the legitimacy of the related signature data by using the public key data corresponding to said secret key data, generates public key certificate revocation list for specifying public key certificate data to be invalidated among said generated public key certificate data, distributes the related public key certificate revocation list to said data providing apparatus, registers and serves usage control policy data indicating the handling of the related content data from said data providing apparatus, and certifies the legitimacy of said usage control policy data in response to a request from said data providing apparatus,

said data providing apparatus performs mutual authentication with said data processing apparatus, encrypts said module using session key data obtained by said mutual authentication, and transmits said encrypted module to said data processing apparatus,

said data providing apparatus provides content data to said data distribution apparatus,

said data distribution apparatus distributes said provided content data and said distributed public key certificate revocation list to said data processing apparatuses, and

said data processing apparatuses verify whether or not public key certificate data of other data processing apparatuses are invalid based on the public key certificate revocation list distributed from said data distribution apparatus, and control the communication with other data processing apparatuses based on the result of the related verification.

203. (Original) A data providing method as set forth in claim 202, wherein said data distribution apparatus has a configuration which makes it difficult to tamper with said public key certificate revocation list distributed from said management apparatus.

204. (Original) A data providing method as set forth in claim 202, wherein

said management apparatus encrypts said public key certificate revocation list using distribution key data and distributes it to said data distribution apparatus and distributes said distribution key data to said data processing apparatus and

said data processing apparatus decrypts said distributed public key certificate revocation list using said distribution key data.

205. (Currently Amended) A data providing method using a data providing apparatus, data distribution apparatus, a plurality of data processing apparatuses, and a management apparatus to provide content data, wherein:

a data processing apparatus supplies registration data, indicating an already registered data processing apparatus connected in a predetermined network to which is connected, to said management apparatus, refers to a revocation flag in registration data supplied from said management apparatus and restricts communication with another data processing apparatus having public key certificate data indicated as invalid by the revocation flag,

said management apparatus manages the operation of a data providing service by said data providing apparatus, said data distribution apparatus, and said data processing apparatuses, generates and manages public key certificate data of public key data corresponding to secret key data for when a data processing apparatus generates signature data indicating legitimacy of data using its own secret key data when supplying data to another apparatus, generates public key certificate revocation list for specifying public key certificate data to be invalidated among said generated public key certificate data, stores the related public key certificate revocation list, generates new registration data by setting said revocation flag in said registration data supplied from data processing apparatuses based on the related public key certificate revocation list, distributes the related generated registration data to said data processing apparatuses, registers and serves usage control policy data indicating the handling of the related content data from said data providing apparatus, and certifies the legitimacy of said usage control policy data in response to a request from said data providing apparatus,

said data providing apparatus provides content data to said data distribution apparatus,

said data providing apparatus performs mutual authentication with said data processing apparatus, encrypts said module using session key data obtained by said mutual authentication, and transmits said encrypted module to said data processing apparatus, and

said data distribution apparatus distributes said provided content data to said data processing apparatuses.

206. (Currently Amended) A data providing method using a data providing apparatus, data distribution apparatus, a plurality of data processing apparatuses, and a management apparatus to provide content data, wherein:

said management apparatus manages the operation of a data providing service by said data providing apparatus, said data distribution apparatus, and said data processing apparatuses, generates and manages public key certificate data of public key data corresponding to said secret key data for when a data processing apparatus generates signature data indicating the legitimacy of data by using its own secret key data when supplying the related data to another apparatus, generates public key certificate revocation list for specifying public key certificate data to be invalidated among said generated public key certificate data, distributes the related public key certificate revocation list to said data providing apparatus, registers and serves usage control policy data indicating the handling of the related content data from said data providing apparatus, and certifies the legitimacy of said usage control policy data in response to a request from said data providing apparatus,

said data providing apparatus performs mutual authentication with said data processing apparatus, encrypts said module using session key data obtained by said mutual authentication, and transmits said encrypted module to said data processing apparatus,

said data providing apparatus provides content data and said public key certificate revocation list to said data distribution apparatus,

said data distribution apparatus distributes said provided content data and said public key certificate revocation list to said data processing apparatuses, and

a data processing apparatus sets a revocation flag in registration data indicating an already registered data processing apparatus connected in a predetermined network to which it is connected based on said distributed public key certificate revocation list and restricts communication with another data processing apparatus having public key certificate data indicated as invalid by the related revocation flag.

207. (Currently Amended) A data providing method using a data providing apparatus, data distribution apparatus, a plurality of data processing apparatuses, and a management apparatus to provide content data, wherein:

said management apparatus manages the operation of a data providing service by said data providing apparatus, said data distribution apparatus, and said data processing apparatuses, generates and manages public key certificate data of public key data corresponding to secret key data for when a data processing apparatus generates signature data indicating the legitimacy of the data by using its own secret key data when supplying the related data to another apparatus, generates public key certificate revocation list for specifying public key certificate data to be invalidated among said generated public key certificate data, distributes the related public key certificate revocation list to said data distribution apparatus, registers and serves usage control policy data indicating the handling of the related content data from said data providing apparatus, and certifies the legitimacy of said usage control policy data in response to a request from said data providing apparatus,

said data providing apparatus performs mutual authentication with said data processing apparatus, encrypts said module using session key data obtained by said mutual authentication, and transmits said encrypted module to said data processing apparatus,

said data providing apparatus provides content data to said data distribution apparatus,

said data distribution apparatus distributes said provided content data and said public key certificate revocation list to said data processing apparatuses, and

a data processing apparatus sets a revocation flag in registration data indicating an already registered data processing apparatus connected in a predetermined network to which it is connected based on said distributed public key certificate revocation list and restricts communication with another data processing apparatus having public key certificate data indicated as invalid by the related revocation flag.

208. (Currently Amended) A data providing method using a data providing apparatus, data distribution apparatus, data processing apparatus, and management apparatus to provide content data, wherein:

said data providing apparatus provides content data and usage control policy data indicating the handling of the related content data to said data distribution apparatus,

said data providing apparatus performs mutual authentication with said data processing apparatus, encrypts said module using session key data obtained by said mutual authentication, and transmits said encrypted module to said data processing apparatus,

said data distribution apparatus distributes said provided content data and said usage control policy data to said data processing apparatus,

said data processing apparatus has a first module for communicating with said data distribution apparatus and a second module for determining at least one of a purchase mode and usage mode of said distributed content data based on said distributed usage control policy data and transmitting log data indicating the log of the related determined purchase mode and usage mode to said management apparatus,

said management apparatus manages the data providing apparatus, data distribution apparatus, and data processing apparatus, registers and serves usage control policy data indicating the handling of the related content data from said data providing apparatus, and certifies the legitimacy of said usage control policy data in response to a request from said data providing apparatus, and

has a settlement function for performing profit distribution processing for distributing the profit obtained accompanied with said data processing apparatus receiving distribution of said content data and purchasing and using said content data to related parties of said data providing apparatus and said data distribution apparatus based on said log data received from said second module and performing settlement based on the result of the related profit distribution processing and a right management function for registering said usage control policy data.

209. (New) A data providing system comprising:

a data providing apparatus that distributes content data and usage control policy data indicating the handling of the related content data to said data processing apparatus,

a data processing apparatus that uses said distributed content data based on said distributed usage control policy data, and

a management apparatus that manages said data providing apparatus and said data processing apparatus,

wherein said data providing apparatus creates said usage control policy data and requests to said management apparatus to certify legitimacy of said usage control policy data, and wherein said management apparatus certifies the legitimacy of said usage control policy data in response to a request from said data providing apparatus by verifying the legitimacy of said usage control policy data and registering authorized usage control policy data in database.